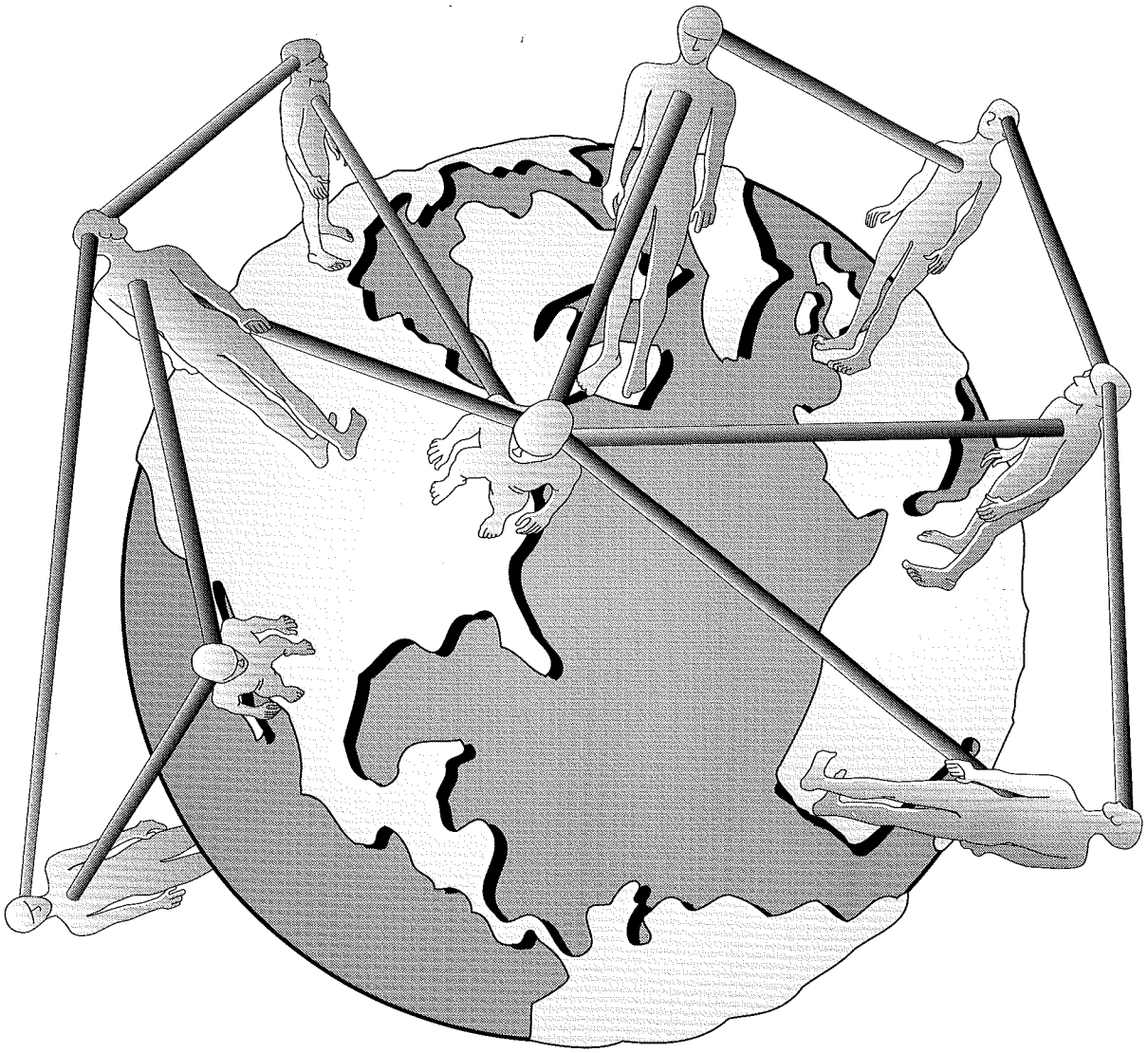
Intertek

Winter, ~~1992~~ 1991 $4.00 Volume 3.3



Virtual Communities

Curtis on MUDs • Reid on IRC • USENET Debate • News

Inter@ctive

editor:
steve steinberg

cover art:
susan tracy
assistance:
travis curl
dave buchwald

FROM: ***Editor***

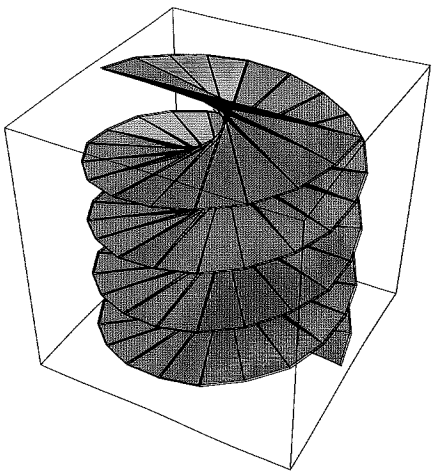
This issue examines four different virtual communities: USENET, Internet Relay Chat (IRC), the computer underground, and Multi-User Dungeons (MUDs). These communities differ from conventional communities in that they are not bound by a geographical locale, and physical presence is not required. Instead, these new communities exist on the global computer network where all interaction is done in ASCII text, and anyone with a computer and a phone line has access. Virtual communities raise new questions about anonymity, gender, and discourse. These questions, as the papers in this issue show, are not merely academic — they are becoming crucial in determining how we will work and play in the 1990s.

steve steinberg

features

discourse

departments



Bury USENET

by Steve Steinberg

The concept of USENET, a global electronic bulletin board on which any person can post messages on topics ranging from nanotechnology to weightlifting and reach other interested people, sounds terrific. It seems like a step towards the magical future which we are all brought up to believe is right around the corner; the future of Hugo Gernsback in which the entire bustling globe is united in productivity and prosperity. But, just as genetic engineering and nuclear power have turned out to cause more problems than they solve, we now see that USENET improves productivity and our quality of life about as much as TV does. True, there are thousands of people who enjoy reading USENET, just as there are millions who enjoy watching TV; however this is not proof of the quaility of the medium but instead is indicative of the lack of alternatives. It is therefore important to understand why USENET fails as a medium so that we can avoid further blunders in this direction.

The three general uses that a medium such as USENET should facilitate are: directed information seeking, browsing, and collaboration. Directed information seeking is when someone is trying to find out a specific piece of information. Browsing is an exploratory information-seeking strategy that is used when the problem is ill-defined or when the user simply wants to become more familiar with an area of knowledge. Lastly, collaboration, for the purposes of this paper, refers to a group of people sharing what they know and posing questions to each other about a particular subject so as to increase the knowledge and ability of everyone involved.

USENET fails at all of these uses, and we can lump the reasons for the failures into three main categories: USENET's asynchronous nature, its small bandwith, and the large amount of noise.

By asynchronous nature I simply mean that communications on USENET is not in real time as it is with a telephone but instead is more like conventional mail. Being asynchronous is not a problem with mail because we communicate with relatively few people, so there are only a small number of letters we need to remember and keep track of. However, when we read hundreds of different messages by different people on different subjects, we quickly get lost and forget what the status is of all the various topic threads. A technique people use on USENET to minimize the drawbacks of asynchronous communications is to begin each message with the relevant portion of the message to which they are replying. This repetition helps to some degree however each message will still only contain some subset of the previous messages (depending on which earlier messages caught the current writer's attention) and so does not give a complete picture of what has been determined on a particular topic. The asynchronous nature of USENET makes collaboration very difficult. A topic will often start with a question and then receive several messages in reply, each of which in turn will spawn several replies. The topic will then quickly degenerate into discussions of trivial points and multiple digressions leaving the poster of the original question, and other readers, more confused than helped. It is the sheer size of USENET, where a topic thread can last for thousands of messages and many months, that makes this problem so intractable.

In these post-MTV proto-multimedia days the idea of people writing to each other seems almost quaint. Indeed one often hears professional writers lament that the death of writing has occurred now that the telephone has supplanted the letter. Hence, it might seem at first blush that USENET is a good thing and will cause the rebirth of the written

USENET NEWSGROUPS

```
alt.activism
alt.alien.visitors
alt.angst
alt.angst.xibo.sex
alt.aquaria
alt.artcom
alt.astrology
alt.atheism
alt.backrubs
alt.bbs
alt.bbs.waffle
alt.beer
alt.binaries.multimedia
alt.binaries.pictures
alt.binaries.pictures.erotic
alt.binaries.pictures.misc
alt.binaries.pictures.taste
alt.birthright
alt.bitch.pork
alt.books.technical
alt.boomerang
alt.boostagogo
alt.brother-jed
alt.buddha.short.fat.guy
alt.cad
alt.cad.autocad
alt.california
alt.callahans
alt.cd-rom
alt.censorship
alt.child-support
alt.co-ops
alt.cobol
alt.colorguard
alt.comp.acad-freedom.news
alt.comp.acad-freedom.talk
alt.comp.compression
alt.config
alt.conspiracy
alt.cosuard
alt.craig.hulsey.rack.rack
alt.cult-movies
alt.culture.electric
alt.cyb-sys
alt.cyberpunk
alt.cyberspace
alt.cybertoon
alt.dads-rights
alt.dcom.catv
alt.dcom.telecom
alt.desert-shield
alt.desert-storm
alt.desert-storm.facts
alt.desert-thekurds
alt.desert.toppings
alt.destroy.the.earth
alt.devilbunnies
alt.dice-man
alt.discrimination
alt.dreams
alt.drugs
alt.drugs.usenet
alt.education.disabled
alt.education.distance
alt.emusic
alt.ensign.wesley.die
alt.ernie-pook
alt.evil
alt.exotic-music
alt.exploding.kibo
alt.fan.BIFF
alt.fan.albedo
alt.fan.bill-fenner
alt.fan.bruce-becker
alt.fan.dan-quayle
alt.fan.dave_barry
alt.fan.frank-zappa
alt.fan.furry
alt.fan.harry-mandel
alt.fan.howard-stern
alt.fan.john-palmer
alt.fan.mike-jittlov
alt.fan.monty-python
alt.fan.pern
alt.fan.rush-limbaugh
alt.fan.suicide-squid
alt.fan.tna
alt.fan.tom_peterson
alt.fan.warlord
alt.fandom.cons
```

```
alt.fandom.misc
alt.fax
alt.fax.bondage
alt.finals.suicide
alt.fishing
alt.flame
alt.flame.abortion
alt.flame.eternal
alt.flame.hirai.cs.dork
alt.flame.pizza.greasy
alt.flame.psu
alt.flame.psuvm
alt.flame.sean-ryan
alt.flame.spelling
alt.flame.those.nasty.little
alt.folklore.computers
alt.folklore.urban
alt.foolish.users
alt.forgery
alt.fractals
alt.fractals.pictures
alt.french.captain.borg
alt.fusion
alt.gambling
alt.games.galactic-bloodshed
alt.games.gb
alt.games.torg
alt.games.xtrek
alt.good.news
alt.gorby.coup.coup.coup
alt.gothic
alt.gourmand
alt.graffiti
alt.graphics.pixutils
alt.great-lakes
alt.hackers
alt.half.operating.system.delay.
alt.hash.house.harriers
alt.homosexual
alt.horror
alt.hotfut
alt.humor.oracle
alt.hypertext
alt.individualism
alt.industrial
alt.iraqi.dictator.bomb.bomb.
alt.irc
alt.irc.sleaze
alt.irc.sleaze.mark
alt.is.too
alt.ketchup
alt.kids-talk
alt.lang.asm
alt.lang.cfutures
alt.lang.intercal
alt.lang.ml
alt.lang.teco
alt.lawyers.sue.sue.sue
alt.letter.chain
alt.magic
alt.magick
alt.maroney
alt.messianic
alt.missing-kids
alt.models
alt.mothers
alt.msdos.programmer
alt.mud
alt.mud.lp
alt.mud.tiny
alt.my.crummy.boss
alt.my.head.hurts
alt.national.enquirer
alt.native
alt.newsgroup.creators.dork.dork.dork
alt.nick.sucks
alt.nodies
alt.noise
alt.pagan
alt.paranormal
alt.party
alt.peeves
alt.personals
alt.personals.bondage
alt.personals.misc
alt.politics.homosexuality
alt.postmodern
alt.privacy
alt.prose
alt.prose.d
alt.psychoactives
alt.putz.bickering.whining.weiner
alt.rap
alt.rap-gdead
alt.recovery
alt.religion.computers
alt.religion.emacs
alt.religion.scientology
```

letter. Unfortunately, as someone who has waded through tens of thousands of USENET messages, I can say with some certitude that this rebirth has not occurred, nor does it appear likely. To write clearly and concisely requires skill as well as time. Because most people lack one or the other of these requirements, messages posted to USENET are usually confusingly worded, difficult to read, and prone to misinterpretation. This is what I was referring to when I said in the beginning that one of the fundamental problems with USENET is its small bandwith. When we express our feelings on a subject or explain a detailed technical matter, we usually use many cues and tools in order to make ourselves understood. These include tone of voice, body language, and pictures or diagrams. When we try instead to compress our thoughts into 80-column ASCII, we leave behind many of the nuances. This makes any use of USENET—whether it be searching or collaborating—difficult since we often do not understand what a message is really trying to say.

One solution to the problem of small bandwith that seems likely to catch on in a big way soon (it already has to some degree) is to allow graphics to be viewed over USENET. This would allow a user to include a drawn or digitized picture inside the message he or she posts. Multimedia messages seem like a good idea, and you can easily imagine the good uses possible such as diagrams to clearly indicate how something works. However, I have no doubts, based on how people have used USENET so far, that the main results would be an outbreak of pornography and a rash of garish signatures.

Reading USENET is like drinking from a firehose, you'll get very wet but you probably will still be thirsty. The problem is that there are thousands of messages posted each day, but only a few of these will be of interest to any one reader. Searching through this haystack of messages is a tedious and laborious task with no sure method of success. Many people end up spending (some would say wasting) several hours a day reading USENET in order to find the few items of interest and importance to them. What further complicates the task of searching for information, making it near impossible as well as unpleasant, is the huge amount of noise — lengthy messages which say nothing useful, messages that are personal attacks on someone, and messages that are plain wrong.

Anyone with access to a UNIX machine that has a USENET feed can post a message on any subject, no matter how unqualified the author may be. The result is usually chaotic and unenlightening. Even when the poster is humble enough to prefix his or her message with "I'm no lawyer /scientist /doctor but...", a clear signal that we may save time and skip this message, we only continue on to ten more messages by other unqualified people berating the first poster for inaccuracies. The dichotomy which is being exposed here is between a medium which informs and a medium for general discussion. If we think USENET should be the former, then there is no place for messages by unqualified people. If USENET should be for discussion, then indeed anyone should be allowed to offer their opinion. Unfortunately USENET isn't very good at this either due to the phenomena known as "flaming" in which users attack other persons' views far more quickly and violently than would occur with any other medium. Because users are safely hidden behind their terminal, and can not see who they are talking to, standard social customs concerning conversation do not seem to apply. The result is that even the most innocent comment can provoke typed vitriol from someone who feels offended. Flaming is undoubtedly the most virulent form of noise, and there is nothing more unpleasant than having to wade through messages of infantile bickering. So, although USENET tries to be both a medium for informing as well as discussion, it succeeds at neither.

The concept of a moderated newsgroup is a simple solution to the noise problem, but it leads to a problem of a different kind. In a moderated newsgroup a user sends messages to the person in charge of the newsgroup, and this moderator then picks only the messages he or she feels are relevant. Sometimes this works well as in the often cited

example of Peter Neumann's RISK digest. However, there is the insidious danger of moderator bias. The specter of this problem has risen in conjunction with the TELECOM digest which is moderated by the rather opinionated Patrick Townsend. Whether Townsend actually censors messages he disagrees with is not important. The perception—and the possibility—are there.

To summarize, USENET's asynchronous nature makes collaboration difficult, its small bandwith makes messages difficult to understand and easy to misinterpret, and the high amount of noise makes searching for interesting messages time consuming and unpleasant.

I wish I could end by presenting five easy steps to improve USENET. Unfortunately, the only ones which seem feasible, such as news readers which use artificial intelligence techniques to filter out noise, are merely stopgap measures which do not address all of the fundamental problems. Before we can fix USENET we must first understand how we learn and how groups work together. Until this has been determined our tools are as likely to hinder our productivity as they are to help us. As has been amply demonstrated by television over the last fifty years, some mediums, no matter how much of a good idea they may seem, just don't work. I hope we quickly learn to see USENET as a noble but failed experiment so that we can research other directions in order to find new mediums that really do enhance our communications and our quality of life.

■

RESPONSES:

Somewhere between the intimacy of island universe conferencing systems like the WELL (an electonic bulletin board in California) and the anarchic ocean of USENET lies the future of computer conferencing. USENET's problems are legion and unlikely to go away. What may succeed are new generations of software and conferencing systems built upon the lessons and experience, both positive and negative, of a multiplicity of existing systems.

The WELL works much better than USENET as a source of informed discourse for several reasons:

- It's hosted on a single system, avoiding the lag of distributed systems.
- People pay to be there. This weeds out the single largest source of noise.
- Conferences are all hosted, which acts as a loose control mechanism.
- The management of the system realizes it's running a digital gathering place.

The WELL has problems too. It's insular, its user interface is nothing to be proud of and its telecommunications access cost is excessive if you don't live in the Bay Area.

If these problems were addressed, there's no reason in principle why the example of the WELL couldn't be more widely applied. It wouldn't be USENET, but maybe that's OK.

I envision a system which is on the Internet and thus reachable from anywhere on the Internet, a system which has a graphical user interface (in addition to whatever the hardcore users want), whose conferences are hosted, and which charges a nominal—say a dollar an hour—usage charge. This software may have many separate instantiations, in different locations, serving different needs and interests.

In fact, this is a brief sketch of a design idea for a development project we hope to begin within the Electronic Frontier Foundation (EFF) in 1992.

Mitch Kapor
EFF co-founder

```
alt.restaurants
alt.revisionism
alt.rhode_island
alt.rissa
alt.rock-n-roll
alt.rock-n-roll.metal
alt.rock-n-roll.metal.heavy
alt.romance
alt.romance.chat
alt.rush-limbaugh
alt.save.the.earth
alt.sca
alt.sci.astro.fits
alt.security
alt.security.index
alt.self-improve
alt.sewing
alt.sex
alt.sex.NOT
alt.sex.aluminum.baseball.bat
alt.sex.bestiality
alt.sex.bestiality.hamster.duct-
alt.sex.bondage
alt.sex.boredom
alt.sex.carasso
alt.sex.carasso.snuggles
alt.sex.graphics
alt.sex.homosexual
alt.sex.masterbation
alt.sex.masturbation
alt.sex.motss
alt.sex.movies
alt.sex.pictures
alt.sex.pictures.d
alt.sex.pictures.female
alt.sex.pictures.male
alt.sex.sonja
alt.sex.sounds
alt.sex.wanted
alt.sex.wanted.me-too
alt.sexual.abuse.recovery
alt.sexy.bald.captains
alt.silly.group.names.d
alt.skate
alt.skate-board
alt.skinheads
alt.slack
alt.slack.BoB.dirtbag

sci.aeronautics
sci.aquaria
sci.archaeology
sci.astro
sci.bio
sci.bio.technology
sci.chem
sci.crypt
sci.econ
sci.edu
sci.electronics
sci.energy
sci.engr
sci.engr.chem
sci.environmen
sci.environment
sci.geo.fluids
sci.geo.geology
sci.geo.meteorology
sci.lang
sci.lang.japan
sci.logic
sci.math
sci.math.num-analysis
sci.math.research
sci.math.stat
sci.math.symbolic
sci.med
sci.med.aids
sci.med.physics
sci.military
sci.misc
sci.nanotech
sci.optics
sci.philosophy.meta
sci.philosophy.tech
sci.physics
sci.physics.fusion
sci.psychology
sci.psychology.digest
sci.research
sci.skeptic
sci.space
sci.space.news
sci.space.shuttle
sci.virtual-worlds
comp.admin.policy
comp.ai
comp.ai.digest
```

comp.ai.edu
comp.ai.neural-nets
comp.ai.nlang-know-
comp.ai.philosophy
comp.ai.philosopy
comp.ai.shells
comp.ai.vision
comp.arch
comp.archives
comp.archives.admin
comp.benchmarks
comp.binaries.acorn
comp.binaries.amiga
comp.binaries.apple2
comp.binaries.atari.st
comp.binaries.ibm.pc
comp.binaries.ibm.pc.archives
comp.binaries.ibm.pc.d
comp.binaries.ibm.pc.wanted
comp.binaries.mac
comp.binaries.os2
comp.bugs.2bsd
comp.bugs.4bsd
comp.bugs.4bsd.ucb-
comp.bugs.misc
comp.bugs.sys5
comp.cog-eng
comp.compilers
comp.compression
comp.databases
comp.databases.informix
comp.dcom.fax
comp.dcom.lans
comp.dcom.lans.hyperchannel
comp.dcom.mode
comp.dcom.modem
comp.dcom.modems
comp.dcom.sys.cisco
comp.dcom.telecom
comp.dcom.telecom.digest
comp.doc
comp.doc.techreports
comp.dsp
comp.editors
comp.edu
comp.edu.composition
comp.emacs
comp.fonts
comp.graphics
comp.graphics.avs
comp.graphics.digest
comp.graphics.research
comp.graphics.visualization
comp.groupware
comp.human-factors
comp.hypercube
comp.infosystems
comp.ivideodisc
comp.lang.ada
comp.lang.apl
comp.lang.asm370
comp.lang.c
comp.lang.c++
comp.lang.clos
comp.lang.clu
comp.lang.eiffel
comp.lang.forth
comp.lang.forth.mac
comp.lang.fortran
comp.lang.functional
comp.lang.hermes
comp.lang.icon
comp.lang.idl
comp.lang.idl-pvwave
comp.lang.lisp
comp.lang.lisp.franz
comp.lang.lisp.mcl
comp.lang.lisp.x
comp.lang.misc
comp.lang.modula2
comp.lang.modula3
comp.lang.objective-c
comp.lang.pascal
comp.lang.perl
comp.lang.postscript
comp.lang.prolog
comp.lang.rexx
comp.lang.scheme
comp.lang.scheme.c
comp.lang.sigplan
comp.lang.smalltalk
comp.lang.tcl
comp.lang.verilog
comp.lang.vhdl
comp.lang.visual
comp.laser-printers
comp.lsi
comp.lsi.cad

I have been invited to respond to an article entitled, "Bury USENET." Presumably this means I'm supposed to defend USENET. This is a perplexing idea since USENET will live or die according to whether people find it useful, not what I or the article's author think of it.

The article trots out the usual tired objections (low bandwidth, too much noise, rude posters) but neglects to consider: If USENET is so horrible (we all know that already), why do so many people use it? Well, low bandwidth permits inexpensive connections. Easy connections and posting permit social use of the network. As a written medium, it can transcend language barriers better than oral media. Being asynchronous, it can encompass discussions across countries, time zones, and appointments. Many of its weaknesses are also its strengths.

The advantages of asynchronicity would be lost on someone who thinks of USENET as a BBS system, which it isn't, and never was intended to be. USENET has always been distributed, not centralized, and was inspired by the old ARPANET, not PC bulletin boards. If a BBS is the corner bar and a conferencing system like the WELL is a three-ring circus, USENET is an entire tour by the Grateful Dead. People tend to recognize what they're already familiar with and ignore or complain about the rest, but analogy is not identity (see *Matrix News*, No. 7, October 1991).

The article berates USENET for being too much like television, and not enough, for allowing too easy posting, yet for having too arbitrary moderators, for this and for not the same thing. The important question is not whether USENET has stopped beating its wife yet (it hasn't), but what new and interesting user interfaces and media are being developed. The article complains about difficulty in following threads of conversation, and of having to bypass repetitive follow-ups, but doesn't mention trn or nn, which are user interfaces that address those problems. It asks for directed information seeking but doesn't mention archie, Prospero, WAIS, WWW, netfind, or X.500.

I almost wish the author had been humble enough to prefix the article with a disclaimer that "I'm not familiar with the history of USENET, nor networking technology, nor with current information projects, but...." Yet there are some amusing tidbits, like the assertion that flaming would not occur in any other medium. Oh dear! Those couldn't have been flames I have seen on electronic mailing lists or in science fiction fanzines, or heard on late night talk shows, and there's no point in mentioning Oprah or Geraldo....

USENET has been declared dead many times over the last decade, but a million people are still dancing on its grave.

John S. Quarterman
Matrix Information and Directory Services, Inc.

Steve Steinberg has articulated well a number of breakdowns that people are experiencing with open nets like USENET. I'd articulate the ones cited as follows:

information flooding — people are confronted with large quantities of data in order to find the few items that will enable them to do their work better. Some people spend large amounts of time every day reading newsgroups, email, and bboards. They see this as a waste of time. So do their employers.

"noise" — flurries of opinions, ungrounded assessments, pronouncements by nonexperts, pontifications, blather, falsehoods, myths, flameoffs, public insults, and other texts that have negligible social value are freely shared.

limited bandwidth — it's very difficult to enter into speculations, brainstorms, planning sessions, and related conversations that are important to work. We can't see the others, hear their voice and inflections, watch their body language and posture, etc. We can't react in the moment.

I disagree with Steve's diagnosis that USENET is the problem, but I agree with his implication that USENET can be part of a solution. My diagnosis is that the breakdowns arise from a number of cultural presuppositions that are no longer valid (but we continue

to act as if they were).

For example, we act as if learning is the acquisition of information. So USENET has accumulated a large number of "information sources." But people aren't learning, as Steve pointed out.

Another example is that we act as if work consists of activities among people who exchange messages. So USENET lets people exchange messages. But people are saying they can't get work done over USENET.

Another example is that we act as if people react to messages like computers, i.e., rationally. So USENET has a practice of flaming off (euphemism for grossly offensive public insults). Network users don't see the bad moods and distrust this generates.

In other words, USENET is like a lab dish in which the nasty bacteria of our cultural assumptions can grow unchecked.

These breakdowns are not easy to recover from. They require new assumptions and practices about work and about working together. People will have to share the new assumptions and learn the new practices. This will take time. It has nothing to do with USENET per se, but on the other hand, USENET can take the lead to provide tools and declare policies that will support new practices.

For example, suppose we replace newsgroups with brokers — either people or automated agents (knowbots) that can get you the answers to questions that you have. This might help relieve information flooding.

Suppose we see work as a web of certain types of conversations in which various commitments are made and discharged. Suppose that our email links the messages together by conversation and keeps track of the state of each conversation. Then the email supports the work, and we can move away from email that merely inflames or spreads disinformation. Why not have USENET take the lead to promulgate such mail systems? (Action Technologies' The Coordinator™ is an example.)

Suppose someone (such as yourself) takes the lead and develops a Network Code of Conduct that says, among other things, that flaming, insulting, disinformation, and the like are not helping anyone get their work done, and USENET strongly discourages it. You might say that this would be contrary to the history of USENET, which has no central management. But you don't have to change the management structure of USENET in order to take the lead to develop and promote a Network Code of Conduct. You could probably get the endorsements of organizations like ACM, IEEE, and EFF for such an activity.

Peter J. Denning
George Mason University

I have read with interest Mr. Steinberg's Khrushchevian shoe-wacking threat to bury USENET. His remarks were asynchronous (they were buried for a while under a stack of magazines on my desk), their bandwith was thin (only three pages long, and some of that redundant), and they were noisy. "Bury USENET," indeed. The single coolest thing about USENET is that there's nobody anywhere with the authority, or even the ability, to actually do this.

Anybody who has actually read Hugo Gernsback should realize that Gernsback was not a major fan of decentralized global networks. Gernsback was a technocrat-wannabe who believed the world should be run out of ivory towers by chromedome übermenschen. "Ralph 124C41+" would never have *hung out* on a network; on the contrary, a Gernsback Continuum "network" would be a ruthlessly, optimized pyramid with nobody allowed on it but us techie aristo supergeniuses.

I hear an echo of this when I see Mr. Steinberg sternly promulgating the "three general uses" that a "medium should facilitate." One envisions him efficiently bustling in with his Taylorian stopwatch to stop folks chatting around the water-cooler and "hindering productivity." "Productivity" is not the be-all and end-all of human relationships,

```
comp.lsi.testing
comp.mail
comp.mail.elm
comp.mail.headers
comp.mail.maps
comp.mail.mh
comp.mail.misc
comp.mail.multi-media
comp.mail.mush
comp.mail.sendmail
comp.mail.uucp
comp.misc
comp.msdos.programmer
comp.multimedia
comp.music
comp.newprod
comp.object
comp.org.acm
comp.org.decus
comp.org.eff.news
comp.org.eff.talk
comp.org.fidonet
comp.org.ieee
comp.org.issnnet
comp.org.sug
comp.org.uniforum
comp.org.usenix
comp.org.usenix.roomshare
comp.org.usrgroup
comp.os.aos
comp.os.coherent
comp.os.cpm
comp.os.eunice
comp.os.mach
comp.os.minix
comp.os.misc
comp.os.msdos.apps
comp.os.msdos.desqview
comp.os.msdos.misc
comp.os.msdos.programmer
comp.os.os2
comp.os.os2.apps
comp.os.os2.misc
comp.os.os2.programmer
comp.os.os9
comp.os.research
comp.os.rsts
comp.os.v
comp.os.vms
comp.os.xinu
comp.parallel
comp.patents
comp.periphs
comp.periphs.printers
comp.periphs.scsi
comp.protocols.appletalk
comp.protocols.ibm
comp.protocols.iso
comp.protocols.iso.dev-
comp.protocols.iso.x400
comp.protocols.iso.x400.gateway
comp.protocols.kerberos
comp.protocols.kermit
comp.protocols.misc
comp.protocols.nfs
comp.protocols.pcnet
comp.protocols.ppp
comp.protocols.pup
comp.protocols.snmp
comp.protocols.tcp-ip
comp.protocols.tcp-
comp.protocols.tcp-
comp.protocols.time.ntp
comp.realtime
comp.research.japan
comp.risks
comp.robotics
comp.security
comp.security.announce
comp.simulation
comp.society
comp.society.development
comp.society.folklore
comp.society.futures
comp.society.women
comp.soft-sys.andrew
comp.soft-sys.khoros
comp.software-eng
comp.sources.3b1
comp.sources.acorn
comp.sources.amiga
comp.sources.apple2
comp.sources.atari.st
comp.sources.bugs
comp.sources.d
comp.sources.games
comp.sources.games.bugs
comp.sources.hp48
```

comp.sources.mac
comp.sources.misc
comp.sources.reviewed
comp.sources.sun
comp.sources.unix
comp.sources.wanted
comp.sources.x
comp.specification
comp.specification.z
comp.std.announce
comp.std.c
comp.std.c++
comp.std.internat
comp.std.misc
comp.std.mumps
comp.std.unix
comp.sw.components
comp.sys.3b1
comp.sys.acorn
comp.sys.alliant
comp.sys.amiga
comp.sys.amiga.advocacy
comp.sys.amiga.announce
comp.sys.amiga.applications
comp.sys.amiga.audio
comp.sys.handhelds
comp.sys.hp
comp.sys.hp48
comp.sys.hp48.d
comp.sys.ibm.hardware
comp.sys.ibm.misc
comp.sys.ibm.pc
comp.sys.intel
comp.sys.isis
comp.sys.laptops
comp.sys.m6809
comp.sys.m68k
comp.sys.m68k.pc
comp.sys.mac
comp.sys.mac.announce
comp.sys.mac.hardware
comp.sys.mac.hypercard
comp.sys.next
comp.sys.next.announce
comp.sys.sgi
comp.sys.sun
comp.sys.super
comp.text
comp.text.desktop
comp.text.frame
comp.text.sgml
comp.text.tex
comp.theory
comp.theory.cell
comp.theory.dynamic
comp.theory.info-
comp.theory.self-
comp.unix
comp.unix.admin
comp.unix.aix
comp.unix.amiga
comp.unix.appleIIgs
comp.unix.appleiigs
comp.unix.aux
comp.unix.cray
comp.unix.i386
comp.unix.internals
comp.unix.large
comp.unix.microport
comp.unix.misc
comp.unix.msdos
comp.unix.programmer
comp.unix.questions
comp.unix.shell
comp.unix.sysv286
comp.unix.sysv386
comp.unix.ultrix
comp.unix.wizards
comp.unix.xenix
comp.unix.xenix.misc
comp.unix.xenix.sco
comp.virus
comp.wind.ms
comp.wind.ms.p
comp.women
rec.aquaria
rec.arts.animation
rec.arts.anime
rec.arts.bodyart
rec.arts.books
rec.arts.cinema
rec.arts.comics
rec.arts.comics.marketplace
rec.arts.dance
rec.arts.disney
rec.arts.drwho
rec.arts.erotica
rec.arts.fine

electronic or otherwise. If you want to "facilitate" Advanced Research Projects for the military-industrial complex, then by all means demand that everybody have a doctorate and that they submit all papers, properly footnoted, to a peer-review committee. But don't ask us to read that stuff, because we won't, and you can't make us.

And if you want a group of people to stick to the point and reach serious-minded and accountable collective decisions, then run the group by parliamentary rules of order. Most people would rather hang out and schmooze than attend a subcommittee of Congress; if you're different, forget USENET and watch C-SPAN (even though it's on, horror, TV).

It's true that bulletin-board posts are ill-considered and are not up to elegant pre-telephonic epistolary standards. But adding to the *bandwith* isn't going to help — you'll just get repugnant home-video of portly UNIX freaks. Posts are sloppy because they're *ephemeral.* They're not written in copperplate calligraphy on parchment, sealed with wax, and dispatched by messenger boy. They're practically as ephemeral as spoken words on the telephone—or on CB radio. To invest serious effort in board posts would be perverse. You could drive around with your CB radio, reciting postmodern essays and scientific papers, but what's the point? It doesn't suit the medium. That doesn't mean that CB is a failure and ought to be buried.

It's an amazing accomplishment that a development with the Orwellian potential of ARPANET has become a giant global crabgrass anarchy. It's kind of a tribute to the human spirit, really. Personally, I find most of USENET a waste of time. I agree: it's a firehose. I strongly suspect that most people who really thrive on the network use its e-mail functions to collaborate, and FTP to download large and well-prepared documents; they don't dwell on USENET's rather lame public commentary. But I don't demand that firehoses be scrapped and replaced with canteens. *Intertek* is a canteen: gosh all fishhooks if this journal doesn't actually enhance my communications and my quality of life. That's why I write comments for *Intertek* but never post on USENET.

Bruce Sterling
Author

ACCESS TO USENET:

It is possible to read USENET from most large UNIX systems by using the 'rn' or 'nn' commands, however, many sites only get a subset of the available newsgroups. If you can't get an account on a UNIX system at your school or business, there are a number of public UNIX systems that are accessible via modem. These public systems usually provide access to USENET along with other services. Two such UNIX systems are:

Nyx (Denver) - 303.871.4770 (login as 'new')
ChiNet (Chicago) - 312.283.0559 (login as 'newuser')

Once you are on the net, you may want to ask around (in the appropriate newsgroups) in order to find a public UNIX system which is closer to where you live.

The WELL provides access to USENET as well as to its own discussion groups, however, it is not a free service. For information on getting an account on the WELL, call 415.332.4335, weekdays 9-5 PST. Or call 415.332.6106 at anytime to register via modem.

ELECTROPOLIS:

COMMUNICATION AND COMMUNITY ON INTERNET RELAY CHAT

Elizabeth M. Reid

COMPUTER-MEDIATED COMMUNICATION

Traditional forms of human interaction have their codes of etiquette. We are all brought up to behave according to the demands of social context. We know, as if instinctively, when it is appropriate to flirt, to be respectful, to be angry, or silent. The information on which we decide which aspects of our systems of social conduct are appropriate to our circumstances are more often physical than verbal. We do not need to be told that we are at a wedding, and should be quiet during the ceremony, in order to enact the code of etiquette that our culture reserves for such occasions. In interacting with other people, we rely on non-verbal information to delineate a context for our own contributions. Smiles, frowns, tones of voice, posture and dress tell us more about the social context within which we are placed than do the statements of the people we socialise with. The words themselves tell only half the story—it is their presentation that completes the picture.

These aspects of human communication are taken for granted by us all—yet technology has the potential to challenge them. Computer-mediated communication subverts many of our assumptions about the practice of communication for it relies only upon words as a channel of meaning.[1] This inherent limitation to the medium has several consequences. "Computer-mediated communication has at least two interesting characteristics:" writes Sara Kiesler, "(a) a paucity of social context information and (b) few widely shared norms governing its use."[2] Users of these systems are unable to rely on the conventions of gesture and nuances of tone to provide social feedback. Words, as we use them in speech, fail to express what we really mean once they are deprived of the subtleties of the non-verbal cues that we assume will accompany them. The sense of social context is lost. The standards of behaviour that are normally decided upon by non-verbal cues are not clearly indicated when information is purely textual. Not only are smiles and frowns lost in the translation of synchronous speech to pure text, but factors of environment are unknown to interlocutors. It is not immediately apparent, in computer-mediated communication, what aspects of social etiquette are appropriate.

Given these limitations, how do computer-mediated interlocutors relate to one another? If the problems presented by the medium were insurmountable, then stable systems would not be able to form. Yet they have—computer-mediated communities do exist. One such example is that seen on Internet Relay Chat, the synchronous conferencing facility available on the Internet computer network.

Internet Relay Chat—IRC—allows many hundreds of people to communicate simultaneously. Users issue commands to the IRC program to create 'channels', virtual spaces within which to talk. IRC supports an unlimited number of channels, which are known by any name which users care to create them under. Not all users have access to the same set of commands—there are degrees of privilege. The creator of a channel—the 'channel operator,' or 'chanop'—has the power to control access to that channel, and can 'kick' unwanted people off it. IRC operators—'opers'—maintain the IRC network connections and are able to control access to the entire system and may 'kill' unwanted users.

Kiesler, Siegel and McGuire have described computer-mediated communication as having four distinct features: an absence of regulating feedback, dramaturgical weakness, few social status cues, and social anonymity. IRC is subject to all these forces—yet a coherent system has managed to evolve over the years. Conventional systems for regulating interaction may fall apart when communication is computer-mediated, yet IRC has been in existence for several years, and is (barring technical mishaps) in continuous use. My interest is to describe how this social system works. How do users react to the ways in which computer-mediated communication deconstructs the conventional boundaries defining social interaction? What alternative methods are developed to sustain understanding? How does the electropolis of IRC function as a community?

ANONYMITY

Users of Internet Relay Chat are not generally known by their 'real' names. The convention of IRC is to choose a nickname under which to interact. The nicknames—or 'nicks' as they are referred to—chosen by IRC users range from conventional first names such as 'Peggy' and 'Matthew,' to inventive and evocative pseudonyms such as 'Wintrwolf', 'Pplater', 'LuxYacht', and 'WildWoman.' These names can be changed at will—there is nothing that one IRC user can ascertain about another—beyond the fact that they have access to the Internet—that is not manipulable by that user.

Our efforts at self-presentation usually assume that we cannot change the basics of our appearance. Physical characteristics, although open to cosmetic or fashionable manipulation, are fundamentally unalterable. What we look like, we have to live with. This is, however, not the case on IRC. How an IRC user 'looks' to another user is entirely dependent upon the information they choose to give. It becomes possible to play with identity. The boundaries delineated by cultural constructs of beauty, ugliness, fashionableness or unfashionableness, can be bypassed on IRC. It is possible to appear to be, quite literally, whoever you wish.

The anonymity of interaction in IRC allows users to play games with their identities. The chance to escape the assumed boundaries of gender, race, and age creates a game of interaction in which there are few rules but those that the users create themselves. IRC offers a chance to escape the languages of culture and body.

The changes that a user might make to his or her perceived identity can be small, a matter of realising in others' minds a desire to be younger or more attractive. However, the anonymity of IRC can provide more than a means to 'fix' minor problems of appearance—one of the most fascinating aspects of this computer-mediated fluidity of cultural boundaries is the possibility of gender-switching. While superficial characteristics such as hair colour are relatively easily changed in 'real life,' gender reassignment is a far more involved process. IRC destroys the usually all but insurmountable confines of sex: changing gender is as simple as changing one's nickname to something that suggests the opposite of one's actual gender. It is possible for IRC to become the arena for experimentation with gender-specific social roles:

```
<Upchuck> Umm, I've gender switched once or
twice for about 2 hours or so...
<Marion> how did you find being perceived as
female?
<Upchuck> I did find it mildly irritating that
I should get so much attention and be immedi-
ately fixated as a sex object simply by pre-
tending to be female.[3]
```

The potential for such experimentation governs the expectations of many users of IRC. Gender is one of the more 'sacred' institutions in our society, a quality whose fixity is so assumed that enacted or surgical reassignment has and does involve complex rituals, taboos, procedures, and stigmas—but this fixity becomes problematic on IRC. The attitudes taken by individual users of IRC differ as regards the possibility for gender concealment. Some view it as 'part of the game,' others are hostile toward users who gender switch:

```
<saro> KAREN IS A BOY
<saro> KAREN IS A BOY
<SmilyFace> saro: so?????????
<Karen> yes saro I heard you
<FuzzyB> Takes a relaxed place beside Karen
offering her her favourite drink.
```

Whatever may be the attitude of individual users of the IRC program to such examples of gender experimentation, the crucial point is that it is a possibility inherent to IRC. Exploitation of this potential is an accepted part of the 'virtual reality'—a popular catch-phrase amongst users of the Internet—of IRC. It becomes possible to play with aspects of behaviour and identity that are not normally open to alteration. IRC enables people to deconstruct aspects of their own identity, and to challenge and obscure the boundaries between some of our most deeply felt cultural significances. IRC users show a willingness to accept this phenomenon and to join in the games that can be played within it.

DISINHIBITION

Researchers of human behaviour on computer-mediated communication (CMC) systems have often noted that users of such systems tend to behave in a more uninhibited manner than they would in face-to-face encounters. Sproull and Kiesler state that computer-mediated behaviour "is relatively uninhibited and nonconforming."[4] Rice and Love suggest that "disinhibition" may occur "because of the lack of social control that nonverbal cues provide."[5]

Internet Relay Chat reflects this observation. Protected by the anonymity of the computer medium, and with few social context cues to indicate the 'proper' ways to behave, users are able to express and experiment with aspects of their personality that social inhibition would generally force them to suppress:

```
*bob* by nature I'm shy..
*bob* normally wouldn't talk about such
thingsw if you met me face to face
*bob* thus the network is good..
```

Users of IRC often form strong friendships. Without social context cues to inhibit people—to encourage shyness—computer-mediated interlocutors will often 'open up' to each other to a great degree. Hiltz and Turoff have noted that some users of CMC systems "come to feel that their very best and closest friends are members of their electronic group, whom they seldom or never see."[6] 'Net.romances,' long distance romantic relationships carried out over IRC, can result from the increased tendency for participants in CMC systems to be uninhibited:[7]

```
<Lori> The more we talked, the more we dis-
covered we had in common...
<Lori> I told him that I was starting to get
a crush on him...
<Lori> Anyway, it's grown and grown over the
months.
<Daniel> A few mishaps, but we've overcome
them, to bounce back stronger than ever.
<Lori> And we'll be getting together for 3
weeks at the end of November, to see if we're
as wonderful as we think we are.[8]
```

Such expressions of feeling are not in any way thought to be shallow or ephemeral. Far from being unsatisfactory for "more interpersonally involving communication tasks, such as getting to know someone," as Hiemstra describes researchers of CMC as having characterised the medium, IRC has in this instance fostered an extremely emotional bond between two people.[9] Users of IRC are able to dispense with the conventional boundaries surrounding communication, and cross-cultural exchange, to form deep friendships, even love affairs, with people whom they have never met.

Net.romances display computer-mediated relationships at their most idyllic. However, disinhibition and increased freedom from social norms have another side. Along with increased broad-mindedness and intimacy among some users goes increased hostility on the part of others. 'Flaming,' the expression of anger, insults and hatred, is a common phenomenon. Anonymity makes the possibility of punishment for transgression of cultural mores appear to be limited. Protected by terminals and separated by distance, the sanction of physical violence is irrelevant, although, as I shall discuss later, social sanctions are present and often in a verbal form that apes physical violence. The safety of anonymous expression of hostilities and obscenities that would otherwise incur social sanctions encourages some people to use IRC as a forum for airing their resentment of individuals or groups in a blatantly uninhibited manner:

```
!Venice! Bashers have taken over +gblf... we
could use some help...
!radv*! Comment: -Gay_Bashe:+gblf- FUCK ALL
OF BUTT FUCKING, ASS LICKING, CHICKEN SHIT
BIOLOGICAL DISIASTERS![10]
```

Not all uninhibited behaviour on IRC is either so negative or so positive. Much of the opportunity for uninhibited behaviour is invested by users of IRC in sexual experimentation. The usually culturally enforced boundaries between sexual and platonic relationships are obscured in computer-mediated circumstances. Norms of etiquette are challenged by the lack of social context cues, and the safety given by anonymity and distance allow users to ignore otherwise strict codes regarding sexual behaviour. Conversations on IRC can be sexually explicit, in blatant disregard of social norms regarding the propositioning of strangers:

```
*Han* does this compu-sex stuff really hap-
pen?
Lola-> *Han* *smooch*
*Han* .....are oyu horny today at all ; )?
Lola-> *Han* today? it's the middle of the
night where I am... as for the adjective,
well, do what you can ;-)
*Han* mmmmmm.....when did you last get off?
```

Such behaviour is often referred to as 'net.sleazing.' Sexual experimentation is a popular Internet game, perhaps because the Internet primarily serves educational institutions and thus students who are generally in their late teens or early twenties. Adolescents, coming to terms with their sexuality in the 'real world,' find that the freedom of 'virtual reality' allows them to safely engage in sexual experimentation. Ranging from the aforementioned gender-role switching to flirtation and 'compu-sex,' IRC provides a medium for the safe expression of a "steady barrage of typed testosterone."[11]

Disinhibition and the lack of sanctions encouraging self-regulation lead to extremes of behaviour on IRC. Users express hate, love, intimacy and anger, employing the freedom of the electronic medium to air views and engage in relationships that would in other circumstances be deemed unacceptable. This 'freedom' does not imply that IRC is an idyllic environment. Play with social conventions can indeed lead to greater positive affect between people, as it has between 'Daniel' and 'Lori', and to greater personal fulfillment for some users. It can, however, also create a violent chaos in which people feel 'free' to act upon prejudices, even hatreds, that might otherwise be socially controlled.

SHARED SIGNIFICANCES

"Culture can be understood as a set of solutions devised by a group of people to meet specific problems posed by situations they face in common."[12] In this sense the users of IRC constitute a culture, a community. The measures which users of the system have devised to meet their common problems, posed by the medium's lack of regulating feedback and social context cues, its dramaturgical weakness, and the factor of anonymity, are the markers of their community, their common culture.

Textual substitution of traditionally non-verbal information is a highly stylized, even artistic, procedure that is central to the construction of an IRC community. Common practice is to simply verbalise physical cues, for instance literally typing 'hehehe' when traditional methods of communication would call for laughter. It is a recognised convention to describe physical actions or reactions, usually denoted as such by presentation between two asterisks:

```
<Wizard> Come, brave Knight! Let me cast a
spell of protection on you..... Oooops—wrong
spell! You don;t mind being green for a
while- do you???
<Prince> Lioness: please don't eat him...
<storm> *shivers from the looks of lioness*
<Knight> Wizard: Not at all.
<Bel_letre> *hahahah*
<Lioness> Very well, your excellency. *looks
frustrated*
<Prince> *falls down laughing*.
<storm> *walks over to lioness and pats her
paw*
<Wizard> *Dispells the spells cast on
Knight!*
<Lioness> *licks Storm*
<storm> *Looking up* Thank You for not eating
me!
```

IRC users also have a 'shorthand' for the description of physical condition. They (in common with users of other computer-mediated communication systems such as news and email) have developed a system of presenting textual characters as representations of physical action. Commonly known as 'smileys,' CMC users employ alphanumeric characters and punctuation symbols to create strings of highly emotively charged keyboard art:

:-) or :)	a smiling face, as viewed side-on
:-(or : (	an 'unsmiley': an unhappy face
:-(*)	someone about to throw up
>:-O	someone screaming in fright, their hair standing on end

These 'emoticons,' as they are known on the Internet, are many and various. Although the most commonly used is the plain smiling face—used to denote pleasure or amusement, or to soften a sarcastic comment—it is common for IRC users to develop their own emoticons, adapting the symbols available on the standard keyboard to create minute and essentially ephemeral pieces of textual art to represent their own virtual actions and responses. Such inventiveness and lateral thinking demands skill. Successful communication within IRC depends on such conventions as verbalised action and the use of emoticons. Personal success on IRC depends on the user's ability to manipulate these tools. The users who can succinctly and graphically portray themselves to the rest of the IRC usership will be the ones most able to create a community within that virtual system.

Whether users of IRC are involved in an online fantasy role-playing game, or just feeling happy, the concentration of verbalised physical actions and reactions in their exchanges demonstrates the extent to which users of the IRC system feel it important to create a physical context for their peers to interpret their behaviour within. Verbal statements by themselves give little indication of the emotional state of the speaker, and without physical expression to decode the specific context of statements, it is easy to misinterpret their intent:

```
*Whopper* just kidding..not trying to be
offensive
<Fireship-> *Whopper* didn't assume that you
were...
```

In order for IRC users to constitute a community it is necessary for them to contrive a method to circumvent the possibility of loss of intended meaning of statements. Verbalisation of physical condition is that method. Without some way of compensating for the inherent lack of social context cues in computer-mediated communication, IRC would get no further than the deconstruction of conventional social behaviours. The textual cues utilised on IRC provide the symbols of interpretation—of culture—that are necessary to meet the specific problems posed by CMC. These shared modes of understanding hold IRC users together as members of a community.

The success of any community is dependent upon the degree of voluntary or enforced cooperation between its members. IRC is no exception to this rule. Special problems arise on IRC, not the least of which is the tendency for users to freely express potentially disruptive emotions. Special solutions have been devised to meet these problems—community on IRC is both upheld by convention and enforced by structure.

SOCIAL SANCTIONS

Nicknames are a sensitive issue on IRC. The program demands that each user offer a unique name to the system, to be used in their interaction with other users. It is common for users to prefer and consistently use one nickname, and one of the greatest taboos on IRC is the use of another's chosen nickname. The illegitimate use of nicknames can cause anger on the part of their rightful users and sometimes deep feelings of guilt on the part of the perpetrators. This public announcement was made by a male IRC user to the 'Usenet' newsgroup alt.irc, a forum for asynchronous discussion of IRC:

```
I admit to having used the nickname
"allison" on several occasions, the name of
an acquaintance and "virtual" friend at
another university. Under this nick, I talked
on channels +hottub and +gblf, as well as
with a few individuals privately. This was a
deceptive, immature thing to do, and I am
both embarrassed and ashamed of myself. I
wish to apologize to everyone I misled,
particularly users 'badping' and 'kired'... [13]
```

The physical aspect of IRC may be only virtual, but the emotional aspect is actual. IRC is not a 'game' in any lighthearted sense—it can inspire deep feelings of guilt and responsibility. It is also clear that users' acceptance of IRC's potential for the deconstruction of social boundaries is limited by their reliance on the construction of communities. Experimentation ceases to be acceptable when it threatens the delicate balance of trust that holds IRC together. The uniqueness of names, their consistent use, and respect for—and expectation of—their integrity, is crucial to the development of online communities.

The sanctions available to the IRC community for use against errant members are both social and structural. The degree to which members feel, as 'Allison' did, a sense of shame for actions which abuse the systems of meaning devised by the IRC community, is related to the degree to which they participate in the deconstruction of traditional social conventions. By being uninhibited, by experimenting with cultural norms of gender and trust, 'Allison' became a part of a social network that encourages self-exposure by simulating anonymity and therefore invulnerability. In this case, the systems of meaning created by the users of IRC have become conventions with a terrorizing authority over those who participate in their use. As I shall describe, users of IRC who flout the conventions of the medium are ostracised, banished from the community. The way to redemption for such erring members is through a process of guilt and redemption; through, in 'Allison's' case, a 'public' ritual of self-accusation, confession, repentance, and atonement.

IRC supports mechanisms for the enforcement of acceptable behaviour. Channel operators—'chanops' or 'chops'—have access to the 'kick' command, which throws a specified user out of the given channel. IRC

operators—'opers'—have the ability to 'kill' users, to break the network link that connects them to IRC. The code of etiquette for 'killing' is outlined in the documentation that is part of the IRC program:

> Obnoxious users had best beware the operator who's fast on the /kill command. "/kill nickname" blows any given nickname completely out of the chat system. Obnoxiousness is not to be tolerated. But operators do not use /kill lightly.[14]

There is a curious paradox in the concomitant usage of the words 'obnoxious' and 'kill'. Obnoxiousness seems a somewhat trivial term to warrant the use of such textually violent commands such as /kick and /kill. The word trivialises the degree to which abusive behaviour, deceit, and shame can play a part in interaction on Internet Relay Chat. The existence of such negative behaviour and emotions is played down, denigrated—what is stressed are the measures that can be taken by the 'authorities'—the chanops and opers—on IRC. Violators of the integrity of the IRC system are marginalised, outcast, described so as to seem insignificant, but their potential for disrupting the IRC community is suggested by the emotive strength of the words with which they are punished. The terms 'killing' and 'kicking' substitute for their physical counterparts—IRC users may feel safe from physical threat, but the sanctions of violence are there, albeit in textualised form.

Operators have adopted their own code of etiquette regarding /kills. It is the general rule that an operator issuing such a command should let other operators, and the victim, know the reason for his or her action by adding a comment to the '/kill message' that fellow operators will receive:

```
*** Notice -- Received KILL message for mic
from mgp (massive abusive channel dumping
involving lots of ctrl-gs and gaybashing,
amongst other almost as obnoxious stuff)
*** Notice -- Received KILL message for JP
from Cyberman ((repeatedely ignorning warn-
ings to stop nickname abuse))
```
[15]

Operators have considerable power within IRC. They can control not only an individual's access to IRC but are also responsible for maintaining the network connections that enable IRC programs at widely geographically separated sites to 'see' each other. The issue of whether or not operators have too much power is a contentious one. While operators are careful to present their /killings as justifiable in the eyes of their peers, this is often not felt to be the case by their victims. Accusations of prejudice and injustice abound, and the hierarchical status quo is often summarily re-enforced:

```
!JP! fucking stupid op cybman /killd me--think
ya some kind of net.god? WHy not _ask_ people
in the channle i'm in if I'm annoying them
before blazing away????
*** Notice -- Received KILL message for JP
from Cyberman (abusive wallops)
```

'Kills' can also be seen as unjustified by other operators, and the operator whose actions are questioned by his peers is likely to be 'killed' himself:

```
*** Notice -- Received KILL message for Alfred
from Kamikaze (public insults are not appre-
ciated)
*** Notice -- Received KILL message for Kami-
kaze from dave (yes, but they are allowed.)
```

The potential for tension between operators of IRC is often diffused into a game. 'Killwars,' episodes in which opers will kill each other, often happen. There is rarely overt hostility in these 'wars'—the attitude taken is one of ironic realisation of the responsibilities and powers that opers have, mixed with bravado and humour—an effort to parody those same powers and responsibilities:

```
!puppy*! ok! one frivolous kill coming up! :D
!Maryd*! Go puppy! :*)
*** Notice -- Received KILL message for puppy
from Glee (and here it IS! : )
!Chas*! HAHA : )
*** Notice -- Received KILL message for Glee
from Maryd (and here's another)
*** Notice -- Received KILL message for Maryd
from Chas (and another)
...[fifteen more 'kills' deleted]...
!Alfred! thank you for a marvellously re-
freshing kill war; this completes my intro
into the rarified and solemn IRCop godhood.
```

The ideals of authority and freedom are often in opposition on IRC as the newly invented social conventions of the IRC community attempt to deal with emotions and actions in ways that emulate the often violent social sanctions of the 'real world.' The potential for tension and hostility between users and opers, arising over the latter's use of power, can erupt into anger and abuse. Disagreements between operators can result in the use of their powers against each other. The games that opers play with 'killing' express their realisation of the existence of these elements of tension in the hierarchical nature of IRC culture and serve to diffuse that tension—at least among opers.

THE IRC COMMUNITY

Community on IRC is "created through symbolic strategies and collective beliefs."[16] IRC users share a common language, a shared web of verbal and textual significances that are substitutes for, and yet distinct from, the shared networks of meaning of the wider community. Users of IRC share a vocabulary and a system of understanding that is unique and therefore defines them as constituting a distinct culture. This community is self-regulating, having systems of hierarchy and power that allow for the punishment of transgressors of those systems of behaviour and meaning. Members of the community feel a sense of

responsibility for IRC—most respect the conventions of their subculture, and those who don't are either marginalised or reclaimed through processes of guilt and atonement. The symbolic identity—the virtual reality—of the world of computer-mediated communication is a rich and diverse culture comprised of highly specialised skills, language, and unifying symbolic meanings.

Users of IRC treat the medium as virtually free space, in which they can act out fantasies, challenge social norms, and exercise aspects of their personality that would be inhibited under normal interactive circumstances. The medium itself blocks some of the socially inhibiting institutions that users would, under other circumstances, be operating within. Cultural indicators—of social position, of age and authority, of personal appearance—are relatively weak in a computer-mediated context. They might be inferred, but they are not evident. Internet Relay Chat leaves it open to users to create virtual replacements for these social cues—IRC interaction involves the creation of replacements and substitutes for physical cues, and the construction of social hierarchies and positions of authority. That it is possible for users of IRC to do this is due to the ways in which the medium deconstructs conventional boundaries constraining interaction and conventional institutions of interpersonal relationships. It is this freedom from convention that allows IRC users to create their own conventions and to become a cohesive community.

■

This article was based upon a thesis written in the Department of History at the University of Melbourne (Australia) in 1991. Readers with Internet access might like to FTP the full version, which is available from the following sites:

ftp.ee.mu.oz.au: /pub/text/IRCThesis/
nic.funet.fi: /pub/sci/papers/IRCThesis/
freebie.engin.umich.edu: /pub/text/IRCThesis/
ftp.cs.widener.edu: /pub/cud/papers/

The filenames are electropolis.ps.Z (compressed Postscript file) and electropolis.txt.Z (compressed text file).

Elizabeth M. Reid.
Internet: emr@munagin.ee.mu.oz.au
IRC: Ireshi

NOTES

[1] This may not be the case in the future. Recent advances in 'multi-media' computer applications make the development of CMC systems that incorporate video, audio and textual elements a possibility.

[2] KIESLER, SARA, JANE SIEGEL, and TIMOTHY W. McGUIRE, "Social Psychological Aspects of Computer-Mediated Communication", *American Psychologist*, Volume 39, Number 10, October 1984 (pp. 1123-1134), p. 1126.

[3] All quotes from IRC sessions are taken from logs kept during 1991. These logs were either kept by myself, or given to me by the log-keeper. In all cases names have been changed to preserve anonymity.

[4] KIESLER, SARA and LEE SPROULL, "Reducing Social Context Cues: Electronic Mail in Organizational Communication" in *Management Science*, Volume 32, Number 11, November 1986 (pp.1492-1512), p.1498.

[5] RICE, RONALD E. and GAIL LOVE, "Electronic Emotion: Socioemotional Content in a Computer-Mediated Communication Network" in *Communication Research*, Vol.14 No.1, February 1987 (pp. 85-108), p.89.

[6] HILTZ, STARR ROXANNE and MURRAY TUROFF, *The Network Nation: Human Communication via Computer*, Addison-Wesley Publishing Company, Inc.: Reading, Mass., 1978, p.101.

[7] Users of the Internet often refer to social phenomena occurring on the system by using the format "net.<phenomenon>"—thus 'net.sleazing' and 'net.romance.'

[8] At their request, the original names of the subjects have been quoted.

[9] HIEMSTRA, GLEN, "Teleconferencing, Concern for Face, and Organizational Culture", in M. Burgoon (ed.), *Communication Yearbook 6*, Sage: Berverly Hills, 1982 (pp.874-904), p.880.

[10] Note that these are 'wallop' messages, that is messages written to all operators. Wallops are denoted by the exclamation marks bracketing the speaker's name. +gblf is a popular channel on IRC, so popular that it is in almost—that is, barring technical mishaps—permanent use. The acronym stands for 'gays, bisexuals, lesbians and friends.' Other 'permanent' IRC channels are +hottub, known for flirtatious chat, and +initgame, in which users play games of 'twenty questions'.

[11] BARLOW, JOHN PERRY, "Crime and Puzzlement: Desperados of the DataSphere" electronic manuscript (also published in *Whole Earth Review*, Sausalito, California, Fall 1990, pp.45-57), lines 114-115.

[12] VAN MAANEN, JOHN, and STEPHEN BARLEY, "Cultural Organization: Fragments of a Theory." in P.J. Frost, et. al., (eds.), *Organizational Culture*, Sage: Beverly Hills, 1985 (pp. 31-53), p.33.

[13] Newsgroup alt.irc 28.9.91. By request, I have omitted the name and Internet address of the poster.

[14] Internet Relay Chat, documentation file 'MANUAL.' Copyright (C) 1990, Karl Kleinpaste (Author: Karl Kleinpaste; email karl@cis.ohio-state.edu; Date: 04 Apr 1989; Last modification: 05 Oct 1990).

[15] This log was taken by an IRC operator—these lines consist of 'notices' sent by operators to all other operators online. They are read as follows: the first 'notice' announces that a user named '14982784' has been banished from the IRC system by an operator named 'MaryD', the second that a user named 'mic' was 'killed' by an operator named 'mgp.' '/kill notices' are accompanied by technical information regarding the details of the path over the computer network that the command travelled—these details, being lengthy and irrelevant to my purpose, I have omitted. Note that there is nothing to stop 'killed' users from reconnecting to IRC.

[16] MEYER, GORDON and JIM THOMAS, "The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground" electronic manuscript (also published in SCHMALLEGER, F. (ed.), *Computers in Criminal Justice*, Wyndham Hall: Bristol, Indiana, 1990, pp. 31-67), lines 1145-1146.

ACCESS TO IRC:

In order to use IRC you must have access to a computer which is connected to the Internet and which has the IRC client program installed. You can obtain the IRC client from one of the following anonymous FTP sites:

UNIX client: cs.bu.edu : irc/ircII2.1.4c.tar.Z
plod.cbme.unsw.oz.au : irc/ircII2.1.4c.tar.Z
nic.funet.fi : pub/unix/irc/ircII2.1.tar.Z

MSDOS client: freebie.engin.umich.edu : /pub/irc/clients/MSDOS

REXX VM client: ftp.informatik.uni-oldenburg.de : pub/irc/rxirc

If you are unable to run the IRC client on your computer site, it is possible to access IRC through a remote client by issuing the command 'telnet bradenville.andrew.cmu.edu'. However, this method is not recommended.

In order to use the client you must connect to an IRC server. There are servers throughout the world, and it is best to pick the one which is geographically closest to you. To start, just pick a server from the list below:

bucsd.bu.edu
lyman.pppl.gov
ucsu.colorado.edu
badger.ugcs.caltech.edu
nic.funet.fi
coombs.anu.edu.au
sunsystem2.informatik.tu-muenchen.de

Upon successful connection to IRC, you may want to ask an operator for information on which server would be best for you to use.

More detailed information on using IRC can be obtained by typing '/help' in the IRC client program or by reading the IRC man pages. There is also a USENET discussion group, alt.irc, where a list of servers as well as other helpful information is posted.

(This information is based upon the alt.irc FAQ by Helen Rose.)

UPCOMING CONFERENCE'S

2/7/92	Phoenix, Arizona	
Multimedia Information Systems	✆ 315.443.4445	
2/12/92	London, England	
Cellular Automata	✆ 44.734.661111	×
3/11/92	New York, New York	
Computer Virus & Security Conference	✆ 800.835.2246	❖▼
3/11/92	Hannover, Germany	
Hannover Fair CeBit'92	✆ 609.987.1202	▲
3/18/92	Washington, D.C.	
Computers, Freedom, & Privacy	✆ 202.994.4955	❖▲
3/19/92	Los Angeles, CA	
Virtual Reality and Disabilities	✆ 818.885.2578	❖
3/24/92	Snowbird, Utah	
Data Compression Conference	✆ 617.736.2700	×
5/3/92	Monterey, California	
CHI '92: Human Factors	✆ 415.738.1200	▲
5/11/92	Vancouver, Canada	
Graphics Interface '92	✆ 604.822.8990	❖
5/22/92	Montreal, Quebec	
3rd Conference on Cyberspace	✆ 514.343.5684	❖▼
6/1/92	Tokyo, Japan	
5th Generation Computer Systems	✆ 81.3.3812.2111	×

K E Y

× - Very technical ▲ - Recommended
❖ - General interest ▼ - Not recommended

Dear *Intertek*,

Two comments on the summer issue of *Intertek*:

First, thanks for reprinting Gilmore's coda to the Computers, Freedom & Privacy conference: it was most eloquent and evoked perfectly the hacker—and I do not use that term in a pejorative sense—mythos. I wrote Gilmore right after the conference complimenting him on it, but then again tried to point out that the extra jail cells are not full of drug users, but of major drug dealers and the murderers in their employ. I further tried to point out, as Cliff Stoll does more neatly, that to equate computer use with drug use is a risky and irrational analogy which thoughtful people should avoid. Morris's Internet worm was in no way a victimless event, except perhaps to people who have never had to depend upon system availability or fight for a budget. As the Net has expanded, so has the importance of its being pure and ample: an analogy to the water supply is perhaps more in point. And if authority has to address permissible recreational uses and toxic pollution, there is nothing inherently immoral or arrogant about its doing so effectively. Of course, it would be better if the major players policed themselves. Not much historical basis for that coming about.

Second, the partially blanked-out FBI memo on your inside back-cover certainly has the desired ominous quality that I assume you wanted; but if we consider only the content, I see little cause for concern: the law regards a reasonable expectation of privacy as a prerequisite to the 4th Amendment protection. Here in California, where privacy is a specific Constitutional Right—Article I, section 1—we even have the Davis case forbidding LAPD officers from monitoring college lectures. But a bulletin board is intended for the widest possible audience, and no Court has yet compelled blindfolding or ear-plugging law enforcement alone, when everyone else has access.

You may be interested in checking out the Electronic Communications Privacy Act and the Personal Privacy Acts, 18 USC 2500, 42 USC 2000aa. There are areas of privacy, and then there is a public arena, and the law looks at the objective facts. This is not some hyped up "virtual legality": this is a well-rooted necessity of a legal structure based on democratic processes and balanced power. I think the term "monitored" needs greater consideration: our feds have done stranger things than assigning drones to watch screens unscroll, but that would have to be a cruel and unusual punishment by any civilized standard done on a 24-hour-a-day basis.

And God bless Nick Sade for pointing out (hype list, item 5) that the proponents of the "electronic frontier" are somehow stuck in the era of James T. Kirk and could use a dose of Matt Dillon. Frederick Jackson Turner is dead: if we're going to talk frontier, it would be well to read up on Limerick and Henderson first.

It is not every magazine that prompts this lengthy a response, which observation is intended as a compliment: I am looking forward to your next issue already.

Don Ingraham
Assistant District Attorney
High Tech Crime Team
Alameda, CA

Dear *Intertek*,

The article on scientific ethics by Stacy Steinberg is important and makes a number of crucial points. I think it is clear that scientists must take responsibility for their actions. The response by Dorothy Denning seems to be too much of the blunderbuss knocking down the self-erected straw man. The statement that those without health insurance can get medical treatment is certainly from some world other than ours.

Charles H. Bloomer
Concord, CA

Dear *Intertek*,

In the summer issue of *Intertek* Bruce Sterling mentioned the League for Programming Freedom in a way that gives the wrong idea about its purpose. What was said about the League actually applies to the Free Software Foundation—the League is something entirely different.

The Free Software Foundation aims to give users the freedom to share and change software. We don't do this through political lobbying because too few people agree with this goal. Instead, we simply develop software and share it. It only takes a few good programmers to develop large amounts of useful free software.

The League for Programming Freedom is not concerned with free software at all. It is a grass-roots organization to defend programmers' freedom to write programs by lobbying Congress. The League opposes software patents and copyrighted languages because they make it illegal to write certain kinds of programs, but it has no opinion on how software should be distributed by its author. Most League members are programmers working for software companies; others are students, professors, entrepreneurs, users, or even software companies.

Surveys suggest that the League's view is the majority view among software designers. But confusion between the League and the Free Software Foundation has led many of them to think they disagree with the League when in fact they agree. This confusion has cost the League support that it vitally needs. I hope this letter makes the situation clear.

For more information on the League for Programming Freedom, write to:

League for Programming Freedom
1 Kendall Square #143
PO Box 9171
Cambridge, MA 02139

Richard Stallman
Founder
GNU Project
Cambridge, MA

■

Social Organization of the Computer Underground

Gordon R. Meyer

One way to better understand and anticipate the net communities of the future is to turn to sociology; the study of people in groups. Sociology offers many theories and paradigms that are of use in the study of cyberspace. In this paper my analysis will reflect my background in the study of deviance and crime, and in the theory of differential association as an explanation for deviant behavior.

I don't intend to delve into a discussion of differential association theory, but mention it here as a declaration of my personal bias, and to provide a setting for the discussion that follows. Essentially, and this is enough of an explanation for our purposes here, differential association holds that people commit deviant acts because they define a particular social setting as being one that is favorable to such an act. These "favorable definitions" are different for each individual and are learned through associations with peers and family.

If we proceed from the assumption that our associations with others shape how we interpret meanings and act in society, we can examine relationships in virtual communities to better understand how electronic communities may be affected by the mechanics and peculiarities of cyberspace. In this paper I will examine the computer underground (CU) from a sociological perspective. The CU is appropriate for this type of study as not only does it display most of the characteristics that we would expect a virtual community to exhibit, but as a rule the CU has been quick to adapt technology to achieve new goals, a process that is interesting by itself but also reminds us that technological advances often have unanticipated consequences and can alter the social fabric of our society in many ways.

One approach to studying social groups is to examine their social organization. In social organizational study the focus is on the network of social relations formed among individuals involved in a common activity. In other words, we ask how people organize themselves, socially, to accomplish the purposeful activity that brings them together. In the case of the CU much of the activity occurs in cyberspace and thus provides insight into other communities whose primary interaction is not on a "face-to-face" basis.

In this examination we will be using a typology, developed by Joel Best and David Luckenbill (see Organizing Deviance, 1982), for identifying the social organization of deviant associations. While I do not consider the computer underground to be a criminal community, the fact is that both the stigma and self-imposed descriptions of the community have a deviant or outlaw flavor. Additionally, the legal issues involved in many aspects of CU-related activity, coupled with the current wave of anti-hacker hysteria, do require that a criminal-like discretion and secrecy be a part of CU activities.

The Best and Luckenbill framework suggests that deviant organizations, regardless of their actual type or extent of activity, will vary in terms of complexity of their division of labor, their coordination among organization roles, and the purposiveness with which they attempt to achieve their goals.

Those organizations which display complexity in each of these characteristics are more socially sophisticated than those that are less complex. The scale of organizational sophistication has five levels: loners, colleagues, peers, mobs, and formal organizations. The classification of organizations along this continuum of sophistication is dependent upon the degree to which they exhibit the following four elements:

- Mutual Association
  (do participants associate with one another?)
- Mutual Participation
  (do they participate in their activities together?)
- Division of Labor
  (do the activities require an elaborate division of tasks and roles?)
- Extended Organization
  (do the activities of the group extend over time and space, regardless of current membership in the group?)

These four measure apply to each of the organizational categories in a cumulative fashion. Figure 1, taken from Best and Luckenbill, illustrates how the characteristics combine to form increasingly complex social organizations.

FORM OF ORGANIZATION	MUTUAL ASSOCIATION	MUTUAL PARTICIPATION	DIVISION OF LABOR	EXTENDED ORGANIZATION
Loners	no	no	no	no
Colleagues	yes	no	no	no
Peers	yes	yes	no	no
Mobs	yes	yes	yes	no
Formal Organizations	yes	yes	yes	yes

(1982, p.25) Figure 1

The five forms of organizations, loners through formal organizations, are presented as ideal types, and the characteristics of "organizational sophistication" should be regarded as forming a continuum with groups located at various points along the range. With this in mind, we can briefly examine the CU in terms of each of the characteristics and see how the peculiarities of the virtual community affect the social organization.

MUTUAL ASSOCIATION

Mutual association is the basic indicator of organizational sophistication in deviant associations. Its presence in the

computer underground; the fact that participants associate with one another on the basis of being involved in CU activities; indicates that on a social organization level the CU can be minimally classified as being collegial. Best and Luckenbill discuss some of the advantages of mutual association for unconventional groups:

> The more sophisticated the form of organization, the more likely the deviants can help one another with their problems. Deviants help one another in many ways: by teaching each other deviant skills and a deviant ideology; by working together to carry out complicated tasks; by giving each other sociable contacts and moral support; by supplying one another with deviant equipment; by protecting each other from the authorities; and so forth. Just as [others] rely on one another in the course of everyday life, deviants find it easier to cope with practical problems when they have the help of deviant associates (1982, pp.27-28).

The CU participants face many practical problems in pursuing their activities. For example, in order to pursue their interests requires equipment and knowledge. The problem of acquiring the latter must be solved and, additionally, they must devise ways to prevent discovery, apprehension and sanctioning by social control agents that may define their activities as criminal. The mutual association found in the computer underground is advantageous in obtaining needed information, tools, and support from colleagues.

Various means of communication have been established that allow individuals to interact and obtain support for their activities, regardless of their physical location. As might be expected, the communication channels used by the CU reflect their interest and ability in high-technology, but the technical aspects of these methods should not overshadow the organizational sophistication that they foster.

The computer underground depends on communications technology to provide meeting places for social and "occupational" exchanges. However, phreakers, hackers, and pirates are widely dispersed across the country and often the globe. In order for the communication to be organized and available to participants who live in many different time zones and "work" under different schedules, centralized points of information distribution are required. Several existing technologies — computer bulletin boards, voice mail boxes, "chat" lines, and telephone bridges/loops — have been adapted by the CU for use as communication points.

In addition to providing a general community structure around which the CU can gather, individual BBS's and the like can harbor smaller, more sophisticated communities with stronger ties of membership and belonging. Any individual that frequents a bulletin board or other communication point can be considered a member of that community, simply by virtue of their attendance. However, "elite" boards, such as are often found in the pirate community, can strengthen these bonds by allocating specific roles to members and requiring levels of participation to retain membership.

However, if mutual participation on a system—regardless of whether it is a BBS, voice mail box (VMB), or chat line—is the only requirement for association with the community, it is likely to remain an unstable and transitory type of organization. Electronic communication offers several advantages, but it also allows participants to sever ties to the community at will simply by cessation of access to the community gathering point. Additionally limiting interaction to "handles only," where real identities are not known or exchanged, increases the ease in which such relationships can be severed. But even with this in mind, it is clear that phreakers, hackers, and pirates are more organizationally sophisticated than loners. They have adopted existing methods of communication, consistent with their skills in high technology, to form a social network of loosely associated individuals that allows for the exchange of information and socializing with others.

Electronic communication offers several advantages, but it also allows participants to sever ties to the community at will.

MUTUAL PARTICIPATION

The social network of the computer underground provides the opportunity for colleagues to form cooperative working relationships with others, thus moving the CU towards a more sophisticated form of social organization. Their social outlets and means for informational exchange bring the CU community together as deviant colleagues. Their relationships fit quite well into the Best and Luckenbill typology of collegial associations:

> The relationship between deviant colleagues involves limited contact. Like loners, colleagues perform their deviant acts alone. But unlike loners colleagues associate with one another when they are not engaged in deviance... In effect, there is a division between two settings; on stage where an individual performs alone; and backstage, where colleagues meet (cf Goffman). In their backstage meetings, colleagues discuss matters of common interest, including techniques for performing effectively, common problems and how to deal with them, and ways of coping with the outside world (1982, p.37).

However, despite the advantages of collegial association, ties among CU participants are weak. Loyalty between individuals seems rare, as the CU is replete with tales of phreak/hackers who, when apprehended, expose identities or "trade secrets" in order to avoid prosecution. These weak collegial ties may be fostered by the anonymity of CU communication methods and the fact that all CU actors are, to some extent, in competition with one another. There are only so many systems with weak security; and once such a system is found, sharing it with

The Street

INDUSTRY UPDATE

Will John F. Akers be remembered as the Mikhail Gorbachev of I.B.M.? After one of the most brutal years in I.B.M.'s history, Mr. Akers announced in November a radical new direction for the world's largest computer maker. The company will be reorganized into more than a dozen independent businesses, some of which will compete directly against each other, leaving the new International Business Machines Corporation looking more like a commonwealth than a union. Mr. Akers has said that his goal is to shake the company from its complacency and free individual businesses—including desktop computers, disk drives, and mainframes—from the company's oppressive bureaucracy. These businesses will also be able to form new alliances. The parent company set the example last year by reaching an agreement with Apple Computer, its long time rival in the personal computer business. However, the project faces a great deal of outside skepticism. Early reports are that the action at the new joint venture is political and not technical. And things could get even worse for I.B.M. Some analysts have said that the separate parts of I.B.M. are more valuable than the whole, a view Mr. Akers apparently agrees with. He has recently stated that selling some of the newly independent divisions is possible, and even likely. The challenge for Mr. Akers is to keep parts of the company's culture intact—high technology and a legendary sales force—while paring back on expenses throughout 1992. Whether he can pull this off without destroying what morale is left at the company is questionable. The irony is that Mr. Akers has waited until now to do precisely what the Justice Department spent many years pursuing: breaking up I.B.M.

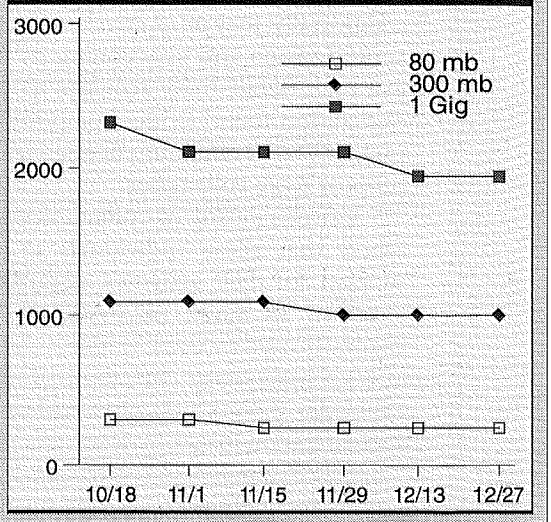
by John Markoff.

HARDWARE PRICES

MEMORY:	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
1 Meg SIMM (<80ns)	$35	35	34	32	31	31	-11.4
4 Meg SIMM (<80ns)	$125	125	125	125	125	125	0.00
HARD DRIVES:							
80mb (<12 ms)	$299	299	259	259	259	259	-13.4
300mb (<12 ms)	$1099	1099	1099	999	999	999	-9.10
1Gig (<15 ms)	$2299	2099	2099	2099	1949	1949	-15.2

Prices based on advertisments in weekly computer magazines.

HARD DRIVE PRICES

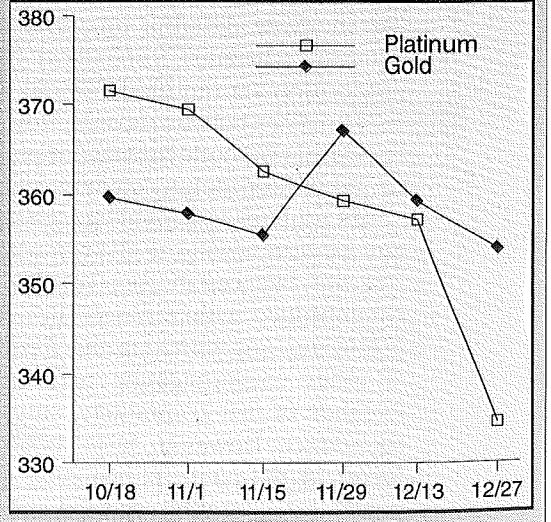


USED COMPUTERS

IBM TYPE:	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
IBM AT 339	$750	750	750	750	750	700	-6.67
IBM PS/2 90	$4300	4300	4300	4300	4100	4000	-6.98
Compaq LTE 286	$1450	1450	1000	1000	1000	1000	-31.03
APPLE:							
Macintosh SE	$950	950	950	950	1000	950	0.00
Macintosh IIX	$3500	3500	3100	3100	3000	3000	-14.29
Macintosh IIFX	$5200	5200	4600	4600	4500	4600	-11.54

Information from the Boston Computer Exchange (BoCoEx).

GOLD & PLATINUM PRICES



HARD CURRENCY

METALS:	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
Platinum (ounce)	$371.60	369.54	362.70	359.40	357.10	334.40	-10.01
Gold (troy ounce)	$359.60	357.75	355.50	367.10	359.35	354.05	-1.54
Silver (troy ounce)	$4.10	4.105	4.075	4.080	3.820	3.85	-6.10
DRUGS:							
Cocaine (1/8 ounce)	$130	130	140	140	125	130	0.00
MDMA (gram)	$115	120	130	120	150	150	+30.4
Ketamine (gram)	$75	75	*na*	*na*	100	90	+20.0

Compiled from buyers and sellers on the west coast.

& Market

STOCK MARKET INDEXES

	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
Germany (DAX)	1563.23	1573.55	1629.37	1566.57	1558.34	1563.59	+0.02
Japan (Nikkei)	24894.82	25044.24	24099.18	23687.35	22754.90	22437.20	-9.87
Switzerland (CrSuisse)	511.00	485.80	492.80	457.50	443.80	443.80	-13.15
United Kingdom (FT-SE)	2610.00	2539.40	2546.60	2420.20	2451.60	2418.70	-7.33
United States (DJIA)	3077.15	3056.35	2943.20	2894.68	2914.36	3101.52	+.79

INDUSTRY GROUPS (Value)

TECHNO:	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
Aerospace/Defense	399.30	403.21	384.26	373.25	367.77	389.18	-2.53
Communications	227.44	230.90	227.47	221.41	222.66	235.73	+3.64
Computers	235.46	229.63	220.96	221.05	220.65	232.45	-1.28
Software	1956.00	2038.02	2013.69	2027.32	2133.52	2321.07	+18.66
OTHER:							
Media	434.65	427.98	420.73	400.60	415.96	438.87	+0.97
Recreation	269.53	275.62	267.69	261.34	261.94	270.50	+0.36
Pharmaceuticals	647.41	674.03	654.27	655.98	681.13	748.23	+15.57

SPECIFIC STOCKS

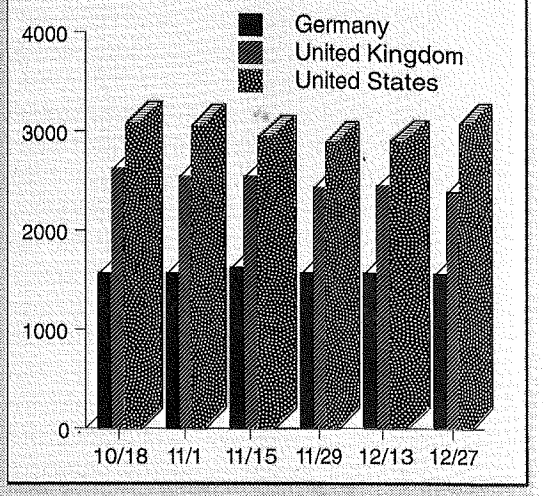
AMERICAN:	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
Apple	$55	51	50	50.75	50.375	55	0.00
AutoDesk	$47.875	42	38.5	33	34.25	32	-33.16
Genentech	$32.75	36	33	31.125	31.375	31.625	-3.44
Intel	$44	41.875	41	41	44.25	47.5	+7.95
Lockheed	$41.375	45.5	45.25	43.75	43.375	44	+6.34
Pacific Telesis	$40.375	32.5	42	39.75	42.25	42.625	+5.57
OTHER:							
Mitsubishi Elec. (yen)	639	637	600	570	589	560	-12.36
NEC (yen)	1270	1290	1160	1150	1190	1140	-10.24
Nintendo (yen)	13600	13700	12400	11700	12100	11500	-15.44
Sandoz (francs)	2410	2390	2570	2370	2420	2430	+0.83

FOREIGN EXCHANGE (Foreign Currency in U.S. $)

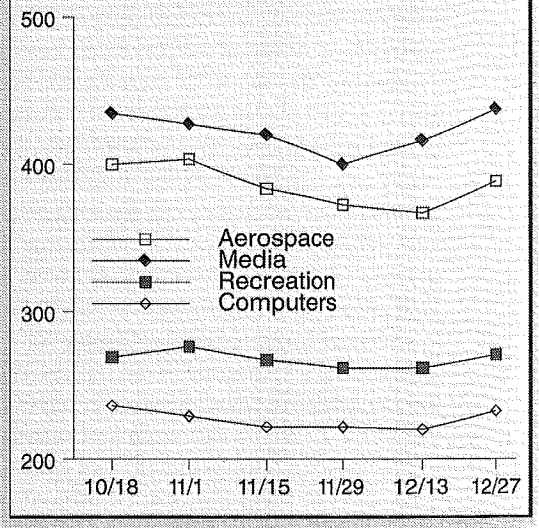
	10/18	11/1	11/15	11/29	12/13	12/27	%Δ
Britain (pound)	$1.7275	1.7660	1.7770	1.7678	1.8160	1.8750	+8.54
Germany (mark)	$0.5929	.6083	.6150	.6154	.6299	.6588	+11.1
Japan (yen)	$0.007716	.007713	.007716	.007701	.007756	.007949	+3.02
Switzerland (franc)	$0.6782	.6932	.6940	.6974	.7132	.7405	+9.19
Taiwan (dollar)	$0.038285	.038476	.038670	.038820	.039216	.039262	+2.55
ECU[1]	$1.21147	1.22619	1.25163	1.24947	1.28350	1.34240	+10.8

[1] European Currency Unit is based on a basket of community currencies.

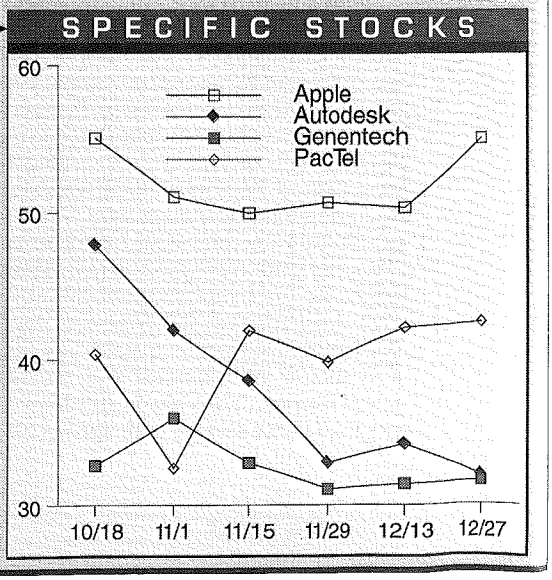
STOCK MARKETS



INDUSTRY GROUPS



SPECIFIC STOCKS



others will virtually ensure that the hole will be sealed when the increased activity is noticed.

As Best and Luckenbill have observed, in order to remain in a collegial relationship individuals must be able to successfully carry out operations alone. Likewise, in order to sustain a career in the CU, one must pursue and collect information independent of what is shared on the communication channels. Despite the association with other phreakers and hackers, the actual performance of the phreak/hacking act generally remains a solitary activity.

That is not to say, however, that phreaks and hackers never share specific information with others. CU bulletin board systems frequently have differentiated levels of access where only highly regarded individuals are able to leave and read messages. The opportunity to share information with selected colleagues often leads to the formation of cooperative "working groups." These partnerships are easily formed as the structure of mutual association in the CU creates a means wherein "talent" can be judged by past interactions, longevity in the field, and mutual interests. When allegiances are formed, the CU actors begin "mutually participating" in their acts, thus becoming "peers" on the scale of social organizational sophistication.

Mutual participation, as originally defined by Best and Luckenbill, is exhibited by actors sharing in the same deviant act while in the physical presence of one another. However, the scale of measurement was devised from the study of traditional "deviant" associations (e.g., street gangs, prostitutes, etc.) where face-to-face interaction is required. The technology used by the CU negates this requirement as actors can be located in different parts of the country. Additionally, "hacking" on a system, by a group of peers, does not require simultaneous participation by all members, as might be required by more traditional forms of deviant behavior. However, Best and Luckenbill's typology is an "ideal type," meaning that empirical evidence does not have to perfectly fit all aspects of the model, and the activities of peers in the computer underground do not fall outside the spirit or intention of their concept of mutual participation. Their description of peer associations is presented here:

> Deviant peers are distinguished from colleagues by their shared participation in deviance. While colleagues carry out their deviant operations alone, peers commit deviant acts in one another's presence. Peers cooperate in carrying out deviant operations, but they have a minimal division of labor, with each individual making roughly comparable contribution. Peer relationships also tend to be egalitarian and informal; some peers may be acknowledged leaders or admired for their skill, but there is no set division of authority. Like colleagues, peers share subcultural knowledge, but peer groups typically provide their members with more support. In addition to cooperating in deviant operations, peers may recruit and socialize newcomers and supply one another with deviant equipment and social support. Thus, the bonds between peers are stronger than those linking colleagues (1982, p.45).

The existence of phreak/hacker groups is commonly known and has been heavily reported in the media. Groups such as the 414's, the Inner Circle, and the Legion of Doom have received a large amount of press after being apprehended or suspected of various computer break-ins. Such work groups are also found in the realm of software piracy, particularly in Europe where several groups act as conduits for foreign software to the United States, and vice versa. However, the media has probably overstated the "threat" that such groups actually pose.

The actual performance of the phreak/hacking act generally remains a solitary activity.

DIVISION OF LABOR

The next organizational measure is that of division of labor. As the title implies, this category refers to the manner in which specific tasks are assigned and carried out by the group of peers.

While it is true that many CU groups are composed of members with talents in specific areas, such as VMB hacking, Unix, DEC, and so on, generally speaking there is not an enforced nor sophisticated division of labor in terms of duties and responsibilities to the group.

Some CU groups may exhibit some of the characteristics of this area but not to the extent that would allow them to be accurately characterized as "mobs." For comparison purposes, recall that these categories are defined on the basis of real-life, deviant organizations; and the name "mob" is an apt description for organizations at this level. Those familiar with the archetypical mobster movie will have no doubt that the CU does not fit this description. A CU group that reached this level of organization would exhibit a hierarchical membership with specific responsibilities, roles, and duties associated with membership. I know of no CU group where this is the case.

FORMAL ORGANIZATION

As the final element of the typology, formal organization is a measurement which indicates a very sophisticated, deviant association. The key element to be emphasized in this area is that a formally organized association will continue to exist over time, regardless of individual members and leadership. A formal organization will have codified rules for behavior, settlement of disputes, and accession of leadership.

Since the scale of sophistication is cumulative, with the prior measure needing to be achieved before the next can be obtained, it is obvious that CU associations do not fall into this category since they do not possess the division of labor required for the previous measure.

CONCLUSION

This examination has discussed the extensive social network used by the computer underground for the exchange of resources and mutual support. As the overall net-community grows, and we become more dependent on electronic communication for daily interaction, we may see some of what the CU displays today in tomorrow's cyberspace.

In the CU, contact outside of cyberspace is generally limited, and the anonymity of the net, as well as the stigma attached to CU activities, inhibit the growth of stronger social ties. Currently it is up to the individual to maintain contact and good will with others. Behind the cloak of a pseudonym or impersonal electronic mail address it is possible to engage and disengage from social contacts at will, a process that does not foster cultural and group unity. This trait alone may be difficult to overcome in a cyberspace world.

The very structure that permits mutual association among CU participants also encourages some to form working relationships, thus acting as peers by mutually participating in CU activities. Peers organized in this manner share in their deviance, organizing informally with little division of labor or set division of authority. These peer associations provide support to members, and can provide socialization and recruitment functions for newcomers.

The establishment of work groups, through mutual participation, suggests that though the computer underground is largely organized as a network of colleagues, it is also, to some degree, a social organization of peers. This trait can probably be expected to continue as the net becomes more and more popular. Separation into smaller associations will be necessary to focus on specific tasks, projects, or even subjects. A current example is USENET which is split into many newsgroups, each focusing on various special interests.

The organizational sophistication of a group has an effect on its future and the types of resources on which its members can draw. Because CU members are mutually associated, they are able to turn to colleagues for advice and support with various problems. However, at the collegial level they are left to enact the solutions independently. Whether they are successful in doing so will determine if they choose to remain active in the computer underground. Most research suggests that involvement in the CU is short in duration unless success in early phreak/hack attempts is obtained. As long as the CU remains organized as a collection of colleagues, this trend will continue.

Additionally, as the computer and telephone industries become more sophisticated in preventing the unauthorized use of their facilities, new phreak/hackers are unlikely to succeed in their initial attempts at the act, thus dropping away from the activity and never becoming acculturated to the point where peer relationships can be developed. Likewise, as people new to cyberspace become discouraged due to initial failures with the complexity of navigating the network, they will drop off unless there are support systems to encourage their learning and experimentation.

As organizations approach the peer level of sophistication, a dimension that some members of the CU do display, the knowledge and resources to solve problems and obtain resources is greater. However, even at this level the ties among participants remain weak at best. Although their cooperative ties allow for more sophisticated operations, and somewhat reduce the CU's vulnerability to social control agents, it still does not completely eliminate the need for individual success to sustain a CU career. As long as the CU remains at the current level of organizational sophistication, with weak ties and somewhat limited means of support and resource attainment, it will continue to be a transitory and limited "criminal" enterprise.

This realization should be considered by policy makers who desire to further criminalize computer underground activities, or continue to fear the freedoms offered in widespread inhabitance of cyberspace. Given the current organization of the CU, the future social costs of their actions are not likely to expand beyond the current level. There is no evidence to support assertions that the CU is expanding, and the insight provided here shows that it is not likely to do so on a large scale. As more people turn to the network, we are likely to see social structures emerge out of necessity due simply to the number of people involved. However, it may be some time before the culture can create the complex social structures found in other areas of society.

■

References

Best, Joel and David F. Luckenbill. *Organizing Deviance.* New York: Prentice-Hall, 1982.

Becker, Howard S. *Outsiders.* New York: Free Press, 1963.

Berger, Peter L. and Thomas Luckmann. *The Social Construction of Reality.* New York: Anchor, 1966.

Gordon Meyer received his MA in sociology from Northern Illinois University and is the co-editor of the Computer Underground Digest. Portions of this paper may have previously appeared in "The Social Organization of the Computer Underground" MA Thesis, 1989, Northern Illinois University.

Real World Kerberos:

Authentication and Privacy on a Physically Insecure Network

by Ken Duda

In the modern, networked computing environment, a workstation user requires many facilities beyond those of his workstation. In particular, a typical setup places the user's files on a special machine called the file server, and perhaps his electronic mail is received on another machine called the post office. Further, he may engage in electronic messaging, on-line consulting, or other network-based services. When resources are spread across many machines in this way, the environment is said to be *distributed*; while in many ways very convenient for the user, the distributed environment presents new technical challenges, including two of particular importance: authentication and privacy.

A network is said to be physically secure if the network wires are inaccessible, and every machine plugged into the network is trusted and secure. This means that a would-be invader is physically unable to put his own machine on the network or modify the software of machines already on the network. A typical example of a physically secure network is a local-area network of secure UNIX boxes within a small-sized company. A degenerate example is the traditional multi-user UNIX mainframe, on which only trusted staff has access to the machine's internals; the operating system ensures that users are kept electronically isolated. Authentication and privacy are not issues here.

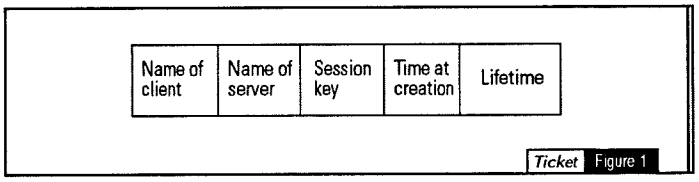
However, as soon as the network grows to any reasonable size, the task of keeping it physically secure becomes impossible. A typical university-wide network, such as the one at the Massachusetts Institute of Technology, is not secure. The global Internet is certainly not secure! In such an environment, two issues arise. First, how does a server establish the authenticity of a request, i.e., ensure that the user, or client, making the request truly is the client he claims to be? Second, how does one prevent so-called promiscuous machines (machines configured to read network packets addressed to other machines) from reading private data? These are the problems of authentication and privacy on a physically insecure network, for which the Kerberos authentication system developed by M.I.T. and Digital Equipment Corporation provides a solution. In this paper I will explain how Kerberos works and then detail some of its insecurities.

HOW KERBEROS WORKS

Kerberos is built around a special, trusted, physically secure machine, called the Kerberos server. The Kerberos server shares secret keys with each client and server on the network. In the case of a user, the secret key is simply the password; for servers or computerized clients, it's a pseudo-random string of bits that serves as a password. The secret key must be protected; if an attacker somehow learns a client's secret key, impersonating the client is effortless. One of the advantages of the Kerberos system is that no other shared secrets are necessary; in particular, no shared secrets are needed between server and client. In contrast, the Appleshare model, for example, requires a shared secret between every server/client pair.

The general strategy is based on a data structure called a Kerberos ticket. Tickets are issued by the Kerberos server. When a client wants to use a service, such as file service, it must obtain a ticket from the Kerberos server and then send it to the file server. The ticket contains the name of the client, the name of the server, and yet another key, a *session key*, generated by the Kerberos server, to encrypt sensitive traffic between the client and the server. In addition, the ticket contains the time it was issued and a *lifetime*, after which it will expire and will no longer be honored (Fig. 1). This way, if a ticket is somehow stolen, it will be of limited usefulness to the attacker. A typical ticket lifetime is around 10 hours.

When a ticket to use a particular service is sent from the Kerberos server to a client, it is encrypted using the service's private key. The session key is sent as well.



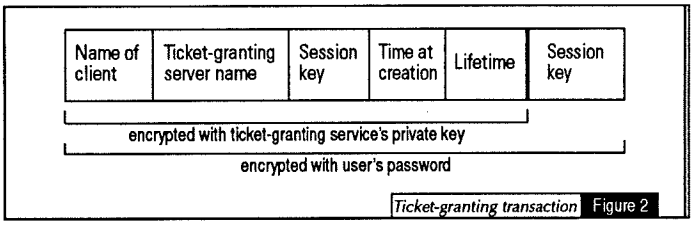
Ticket Figure 1

When the client uses the ticket by sending it to the service, the service attempts to decrypt the ticket, using its private key. If this decryption succeeds, the service can be quite confident that the request is authentic, that is, the named client is who it claims to be. This is because the ticket must have come from the Kerberos server, as it is the only (other) party that knows the service's private key. If the decryption fails, the server knows the ticket was fraudulent.

Given this model, it would seem that a simple attack would be to listen to the net, copy a Kerberos ticket as it goes by, and re-use the exact data, without knowledge of any keys at all. To prevent this attack, the client accompanies the ticket with an *authenticator*, encrypted with the session key. The authenticator contains the current time of day, the name of the client, and the network address of the machine from which the request was issued. The attacker cannot create an authenticator without knowing the session key, which it cannot extract

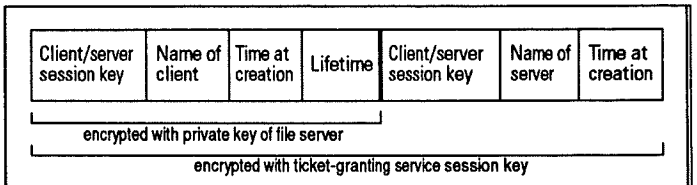
without knowing the service's private key. It cannot use the authenticator later from the machine from which the authentic request was made because the time stamp will be wrong, as authenticators have a five-minute lifetime. A special case is if the attacker is logged onto the user's workstation at the time the request was made; more will be said about this case later. First, we will examine the process in detail, step by step.

Logging In. When a user first logs onto a workstation and enters their user name, the workstation begins the authentication process. It contacts the Kerberos server and requests an initial ticket: a ticket for the Kerberos *ticket-granting service.* This is a service like any other, with its own private key. The Kerberos server forms the ticket, made of a randomly generated session key, the name of the client, the name of the ticket-granting service, the current time, and the ticket's lifetime. This is encrypted, using the ticket granting service's private key. The Kerberos server adds another copy of the session key to the encrypted ticket and encrypts the whole thing, using the user's password (or, in general, the client's private key). This bundle is sent to the client workstation (Fig. 2). Now the workstation asks the user for his password, uses it to decrypt the bundle, and destroys the password from memory as it is advantageous to hold the password in memory for as little time as possible. It then checks to see if the bundle decrypted successfully. If not, the user must have mistyped his password and is so informed. If the user's password was correct, the workstation now has the ticket-granting ticket and Kerberos session key, and can obtain as many tickets from the Kerberos server as are needed. Notice how clever this scheme is: the user's password never had to leave the workstation's memory.



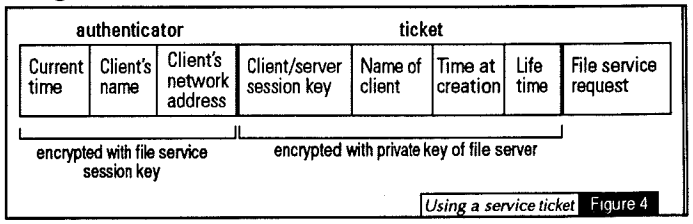
Ticket-granting transaction Figure 2

Obtaining a service ticket. When a client with a ticket-granting ticket wants to authenticate to some other service, such as file service, it must obtain a ticket for that service from the Kerberos server. The server creates an authenticator and encrypts it with the session key from the ticket-granting ticket. The client then sends the authenticator, the ticket-granting ticket, and the name of the file server to the Kerberos server. The Kerberos server decrypts the ticket-granting ticket with the ticket-granting service's private key, revealing the session key; this is used to decrypt and validate the authenticator. Once this has been done, the Kerberos server can be certain of the identity of the client presenting the ticket-granting ticket. It creates the new ticket, made up of a new session key used to encrypt for the client and the file server, the identity of the client, the current time, and a lifetime calculated so that the issued ticket will expire at the same time the ticket-granting ticket does. Then it looks up the private key of the file server and encrypts the ticket with it. The Kerberos server takes the encrypted ticket, the new session key, the name of the service, and a time stamp, and encrypts the whole bundle with the client's ticket-granting service session key (Fig. 3). This is sent back to the client, which decodes it with the session key, checks its integrity, and stores the new file service ticket and session key in a safe place for future use.



Obtaining a service ticket Figure 3

Using a service ticket. To send an authenticated request to the file server, the client creates an authenticator (made of the current time, the client's name, and the client's network address) and encrypts it with the file service session key that came from the Kerberos server with the encrypted file service ticket. It appends the file service ticket and the actual file service request (Fig. 4). For privacy, the file service request could be encrypted with the file service session key as well. The whole bundle is sent to the file server, which first attempts to decrypt the Kerberos ticket with its own private key. From the ticket it extracts the session key and uses it to decrypt the authenticator. It then validates the authenticator by checking to see if the request really came from the host named in the authenticator within five minutes of the authenticator's time stamp. If an attacker faked the source address of the packet, depending on the network layer being used, either a router will refuse to route it (if the host was on the wrong subnet), or the host actually using that address will broadcast an error message. In either case, network authorities will be alerted to the existence of an unusually determined attacker. If all of the validation succeeds, the file server can be confident of the authenticity of the client. Finally, if needed, the server decrypts the file service request itself using the session key. It can send the response back with an authenticator, all encrypted using the session key. The client can be confident of the authenticity of the file server's response because no other machine could know the session key. The server and client have obtained an



Using a service ticket Figure 4

authenticated, private channel without sharing a secret key before the session began. This is the beauty of Kerberos.

KERBEROS INSECURITIES

Kerberos is based on a number of assumptions. The encryption algorithm employed by Kerberos must be safe from cryptanalysis. All server machines must be physically secure. All machines must have their clocks within five minutes of one another's. There must be no way for an attacker to become root on the user's workstation. The system software on each workstation must not be modifiable. Within these constraints, Kerberos has been proven unbreakable. However, I do not find that fact as interesting as the question: what goes wrong when these constraints are not met? What are Kerberos' vulnerabilities in the real world?

The particular encryption algorithm that Kerberos uses is not important. It must only have the property that an attacker knowing the plaintext (unencrypted data) and cyphertext (encrypted data) would still be unable to compute the key. Current Kerberos implementations use the Data Encryption Standard (DES), which is at least popularly believed to have this property. I do not consider this requirement a weakness in Kerberos. However, were an attacker able to compute the key easily from the cyphertext and plaintext, Kerberos would immediately fall apart. The attacker would only have to eavesdrop on the net, read an encrypted ticket, and compute the key required to get the ticket header out of it. This key is the client's private key, which the attacker could use to masquerade effortlessly as that client, "authenticating" to any service at any time.

The server machines must remain physically secure, otherwise it is trivial to become root and thereby compromise the server. Of course, if any given server is physically insecure, only the particular service it offers is compromised. If the physical security of the Kerberos server itself is compromised, however, an attacker could extract from it all private keys for all services and users, resulting in a complete loss of reliable authentication. Thus, any reasonable Kerberos installation keeps the Kerberos server carefully guarded.

The constraints involving workstations open up many more interesting back doors. It is generally accepted that as long as the console/CPU of a workstation is physically accessible, the workstation cannot be truly secure; or, equivalently, there is always some way to get root privileges. In general, you can always boot off of a floppy disk or cartridge tape with your own build of the operating system. Partly to emphasize this point, and partly as a convenience to users, M.I.T. makes no attempt to keep the public workstation root password secret and in fact publishes it (it's `mrroot`, read "Mister Root"). This allows any user to issue any command he wants to the workstation and make arbitrary changes to workstation software, opening up several attacks.

The Simultaneous Login Attack. The easiest attack becomes possible when two users share a workstation (presumably with one logged in remotely). Normally, this is not possible as workstations should be configured to disallow remote logins. However, "clever" users frequently reconfigure the faster workstations to allow remote logins so that they can use their computational power from slower workstations. When I find such a user logged in on my machine with me, I first destroy my own Kerberos tickets to prevent the reverse attack. I then get root privileges and find the file that contains their Kerberos tickets. The file is marked readable only by them (so multiple users can securely share a multiuser machine), but since it is stored on the workstation's local hard disk, root can read it as well. I then copy their Kerberos ticket file over mine. At this point I have all of their privileges and (until their tickets expire) can, for example, read their mail or delete all of their files.

The Background Process Attack. Another method to gain someone else's privileges is to leave a process running as root on a workstation when you log out. A simple example would periodically scan the workstation's drive for Kerberos ticket files and copy them to a holding place when found (to foil their destruction when the user logs out). The attacker could return to the workstation after the user he wished to impersonate had been logged on, become root, and copy the saved tickets over his own. He would then have until the tickets' expiration time to impersonate his victim.

The Trojan Horse. This attack requires programming knowledge and is thus the most difficult. It is also by far the most devastating. It involves modifying the login program (or any other program to which the user types his password, such as the program that obtains ticket-granting tickets). The strategy is frighteningly simple: duplicate the behavior of the original program exactly; but, in addition, rather than destroying the user's password, save it somewhere. Now the attacker can impersonate the user from any workstation at any time, up until the time the user changes his password. At M.I.T., this strategy is particularly easy due to the fact that the source code to the login program is accessible to anyone. I estimate that a skilled programmer who knew nothing more than the login program's location could have a trojan horse in place in a matter of hours and hundreds of passwords within days.

There is no way to completely defend oneself from these attacks. In general, as long as the attacker has root access on your workstation, defense reduces to a cat-and-mouse game reminiscent of copy protection schemes. However, a few simple measures can help defend against many attacks. A security-conscious user always logs on

first as root, checks what processes are running, and then runs a program that compares the workstation's configuration against the standard configuration. The program will also detect if any of the standard programs have been modified. This procedure will catch all of the amateur attackers; however, if you want to be truly secure, you need a secure workstation.

In summary, Kerberos provides authentication and privacy to users and services on a physically insecure network of secure machines. However, it is subject to misuse and (in the insecure workstation model) direct attacks that greatly compromise its power. Nonetheless, for most purposes Kerberos provides a sound solution to network security problems and will serve as a standard for many years to come.

Acknowledgments

My description of how Kerberos works is condensed primarily from the Project Athena Technical Plan, Section E.2.1: Kerberos Authentication and Authorization System, by S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. I recommend this document to those interested in further details of Kerberos.

■

Ken Duda is a student at M.I.T., majoring in Computer Science and Electrical Engineering.

ACCESS TO KERBEROS:

Kerberos is distributed at no charge by M.I.T.'s Project Athena. To retrieve the source code, ftp to ATHENA-DIST.MIT.EDU (18.71.0.38), login as anonymous and then cd to pub/kerberos.

Retrieve README.ftp, it has directions on how to get to the rest of the software (it also contains information on who to contact for export versions of the source code with no encryption routines). If you would like to retrieve documents separately, you can get them from pub/kerberos/doc (documents) or pub/kerberos/man (manual pages). If you prefer the documentation in hardcopy form, send your address and request to "info-kerberos@athena.mit.edu".

Alternatively, you may retrieve the source code and documentation by sending electronic mail to 'archive-server@athena-dist.mit.edu'. The subject line should be 'index krb-code'. This will return an index of the distribution. To retrieve pieces of the distribution, send mail with a subject of 'send krb-code xxxx' where xxxx is the filename as listed in the index. To retrieve documents this way, send a message with subject 'index krb-doc' to get the document index.

There is also a Kerberos mailing list for discussion of Kerberos and related matters. To receive it through email send your request to "kerberos-request@athena.mit.edu." The mailing list can also be read in the USENET newsgroup comp.protocols.kerberos.

RAShYT H GL/GL YM²
———
231/un...At(h)

viscus caldron/dialects of (Av/7 | Abd/7) = QY,/3 N,/0 QOAD⁹/1 +

the pit/Algol/430(=7)/PRQYM   +NBYRILZAA/311 = 3321/Sh... ² + (

the impetus for device/dance, (reduce?
32=0 at 1032, or
spellbound where the train dissolves   annihilation bathtub
(≠ mirror predicate ——————/
asymmetrical trajectory
en vacuum

she was asleep

ATh 401 | & vapor/ars :5

I got to hang these up.

&29 insert,
(reversed?)

hmm?

re : essent/non

I got to hang these up.

Jake Berry

Mudding:
Social Phenomena in Text-Based Virtual Realities

Pavel Curtis
Xerox PARC

Abstract

A MUD (Multi-User Dungeon or, sometimes, Multi-User Dimension) is a network-accessible, multi-participant, user-extensible virtual reality whose user interface is entirely textual. Participants (usually called players) have the appearance of being situated in an artificially constructed place that also contains those other players who are connected at the same time. Players can communicate easily with each other in real time. This virtual gathering place has many of the social attributes of physical places, and many of the usual social mechanisms apply. Certain attributes of this virtual place, however, tend to have significant effects on social phenomena, leading to new mechanisms and modes of behavior not usually seen in 'real life.' In this paper, I relate my experiences and observations from having created and maintained a MUD for over a year.

1 A Brief Introduction to Mudding

> The Machine did not transmit nuances of expression. It only gave a general idea of people—an idea that was good enough for all practical purposes.
>
> E.M. Forster [1]

A MUD is a software program that accepts 'connections' from multiple users across some kind of network (e.g., telephone lines or the Internet) and provides to each user access to a shared database of 'rooms', 'exits', and other objects. Each user browses and manipulates this database from 'inside' one of those rooms, seeing only those objects that are in the same room and moving from room to room mostly via the exits that connect them. A MUD, therefore, is a kind of virtual reality, an electronically represented 'place' that users can visit.

MUDs are not, however, like the kinds of virtual realities that one usually hears about, with fancy graphics and special hardware to sense the position and orientation of the user's real-world body. A MUD user's interface to the database is entirely text based; all commands are typed in by the user, and all feedback is printed as unformatted text on their terminal. The typical MUD user interface is most reminiscent of old computer games like Adventure and Zork [2]. A typical interaction is shown in Figure 1.

```
>look
  Corridor
  The corridor from the west continues to the east here, but the way is
  blocked by a purple-velvet rope stretched across the hall.  There are
  doorways leading to the north and south.
  You see a sign hanging from the middle of the rope here.
  >read sign
  This point marks the end of the currently-occupied portion of the house.
  Guests proceed beyond this point at their own risk.
     -- The residents
  >go east
  You step disdainfully over the velvet rope and enter the dusty darkness of
  the unused portion of the house.
```

A typical MUD database interaction — Figure 1

Three major factors distinguish a MUD from an Adventure-style computer game, though:

- A MUD is not goal oriented; it has no beginning or end, no 'score,' and no notion of 'winning' or 'success.' In short, even though users of MUDs are commonly called players, a MUD isn't really a game at all.
- A MUD is extensible from within; a user can add new objects to the database such as rooms, exits, 'things,' and notes. Certain MUDs, including the one I run, even support an embedded programming language in which a user can describe whole new kinds of behavior for the objects they create.
- A MUD generally has more than one user connected at a time. All of the connected users are browsing and manipulating the same database and can encounter the new objects created by others. The multiple users on a MUD can communicate with each other in real time.

This last factor has a profound effect on the ways in which users interact with the system; it transforms the activity from a solitary one into a social one.

Most inter-player communication on MUDs follows rules that fit within the framework of the virtual reality. If a player 'says' something (using the say command), then every other player in the same room will 'hear' him or her. For example, suppose that a player named Munchkin typed the command,

```
say Can anyone hear me?
```

Then Munchkin would see the feedback,

```
You say, "Can anyone hear me?"
```

and every other player in the same room would see,

```
Munchkin says, "Can anyone hear me?"
```

Similarly, the emote command allows players to express various forms of 'non-verbal' communication. If Munchkin types,

```
emote smiles.
```

then every player in the same room sees,

```
Munchkin smiles.
```

Most interplayer communication relies entirely on these two commands [3].

There are two circumstances in which the realistic limitations of say and emote have proved sufficiently annoying that new mechanisms were developed. It sometimes happens that one player wishes to speak to another player in the same room, but without anyone else in the room being aware of the communication. If

Munchkin uses the whisper command,

```
whisper "I wish he'd just go away..." to Frebble
```

then only Frebble will see,

```
Munchkin whispers, "I wish he'd just go away..."
to you.
```

The other players in the room see nothing of this at all.

Finally, if one player wishes to say something to another who is connected to the MUD but currently in a different and perhaps 'remote' room, the page command is appropriate. It is invoked with a syntax very like that of the whisper command, and the recipient sees output like this:

```
You sense that Munchkin is looking for you in
The Hall. He pages, "Come see this clock, it's
tres cool!"
```

Aside from conversation, MUD players can most directly express themselves in three ways: by their choice of player name, by their choice of gender, and by their self-description.

When a player first connects to a MUD, they choose a name by which the other players will know them. This choice, like almost all others in MUDs, is not cast in stone; any player can rename themselves at any time, though not to a name currently in use by some other player. Typically, MUD names are single words, in contrast to the longer 'full' names used in real life.

Initially, MUD players appear to be neuter; automatically generated messages that refer to such a player use the family of pronouns including 'it', 'its', etc. Players can choose to appear as a different gender, though, and not only male or female. On many MUDs, players can also choose to be plural (appearing to be a kind of 'colony' creature: "ChupChups leave the room, closing the door behind them"), or to use one of several sets of gender-neutral pronouns (e.g., 's/he', 'him/her' and 'his/her', or 'e', 'em' and 'eir').

Every object in a MUD optionally has a textual description which players can view with the look command. For example, the description of a room is automatically shown to a player when they enter that room and can be seen again just by typing 'look.' To see another player's description, one might type 'look Bert.' Players can set or change their descriptions at any time. The lengths of player descriptions typically vary from short one-liners to dozen-line paragraphs.

Aside from direct communication and responses to player commands, messages are printed to players when other players enter or leave the same room, when others connect or disconnect and are already in the same room, and when objects in the virtual reality have asynchronous behavior (e.g., a cuckoo clock chiming the hours).

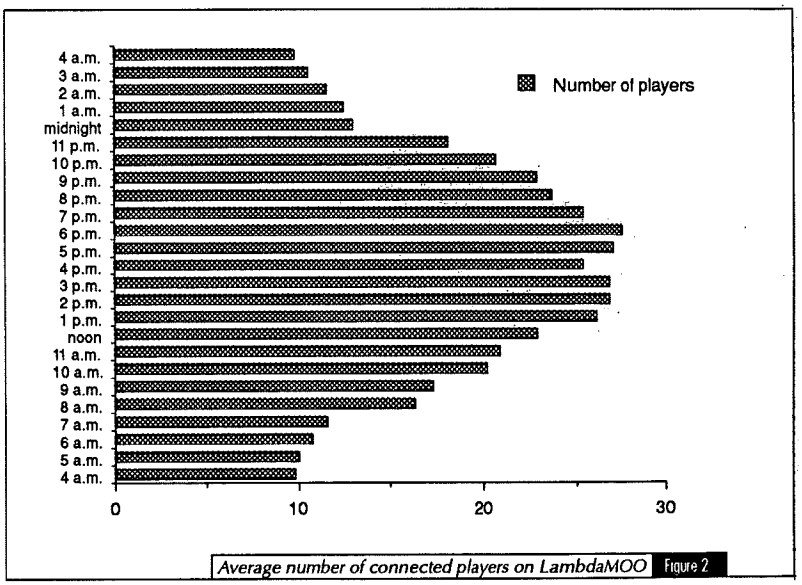
MUD players typically spend their connected time socializing with each other, exploring the various rooms and other objects in the database, and adding new such objects of their own design. They vary widely in the amount of time they spend connected on each visit, ranging from only a minute to several hours; some players stay connected (and almost always idle) for days at a time, only occasionally actively participating.

This very brief description of the technical aspects of mudding suffices for the purposes of this paper. It has been my experience, however, that it is quite difficult to properly convey the sense of the experience in words. Readers desiring more detailed information are advised to try mudding themselves, as described at the end of this paper.

2 Social Phenomena Observed on One MUD

Man is the measure.
E.M. Forster

In October of 1990, I began running an Internet-accessible MUD server on my personal workstation here at Xerox PARC. Since then, it has been running continuously, with interruptions of only a few hours at most. In January of 1991, the existence of the MUD (called LambdaMOO [4]) was announced publicly, via the Usenet newsgroup rec.games.mud. As of this writing, over 2,500 different players have connected to the server from over a dozen countries around the world and, at any given time, over 400 players have connected at least once in the previous week. Recent statistics regarding the number of players connected at a given time of day (Pacific Standard Time) appear in Figure 2.



Average number of connected players on LambdaMOO Figure 2

LambdaMOO is clearly a reasonably active place, with new and old players coming and going frequently throughout the day. This popularity has provided me with a position from which to observe the social patterns of a fairly large and diverse MUD clientele. I want to point

In general, such cruelty seems to be supported by two causes: the offenders believe (usually correctly) that they cannot be held accountable for their actions in the real world, and the very same anonymity makes it easier for them to treat other players impersonally as other than real people.

Wizards. Usually societies cope with offensive behavior by various group mechanisms, such as ostracism, and I discuss this kind of effect in detail in Section 2.3. In certain severe cases, however, it is left to the 'authorities' or 'police' of a society to take direct action, and MUDs are no different in this respect.

On MUDs, it is a special class of players, usually called wizards or (less frequently) gods, who fulfill both the 'authority' and 'police' roles. A wizard is a player who has special permissions and commands available, usually for the purpose of maintaining the MUD, much like a 'system administrator' or 'superuser' in real-life computing systems. Players can only be transformed into wizards by other wizards, with the maintainer of the actual MUD server computer program acting as the first such.

On most MUDs, the wizards' first approach to solving serious behavior problems is, as in the best real-life situations, to attempt a calm dialog with the offender. When this fails, as it usually does in the worst cases of irresponsibility, the customary response is to punish the offender with 'toading'. This involves (a) either severely restricting the kinds of actions the player can take or else preventing them from connecting at all, (b) changing the name and description of the player to present an unpleasant appearance (often literally that of a warty toad), and (c) moving the player to some very public place within the virtual reality. This public humiliation is often sufficient to discourage repeat visits by the player, even in a different guise.

On LambdaMOO, the wizards as a group decided on a more low-key approach to the problem; we have, in the handful of cases where such a severe course was dictated, simply 'recycled' the offending player, removing them from the database of the MUD entirely. This is a more permanent solution than toading but also lacks the public spectacle of toading, a practice none of us were comfortable with.

Wizards, in general, have a very different experience of mudding than other players. Because of their palpable and extensive extra powers over other players, and because of their special role in MUD society, they are frequently treated differently by other players.

Most players on LambdaMOO, for example, upon first encountering my wizard player, treat me with almost exaggerated deference and respect. I am frequently called 'Sir,' and players often apologize for 'wasting' my time. A significant minority, however, appear to go to great lengths to prove that they are not impressed by my office or power, speaking to me quite bluntly and making demands that I assist them with their problems using the system, sometimes to the point of rudeness.

Because of other demands on my time, I am almost always connected to the MUD but idle, located in a special room I built (my 'den') that players require my permission to enter. This room is useful, for example, as a place in which to hold sensitive conversations without fear of interruption. This constant presence and unapproachability, however, has had significant and unanticipated side effects. I am told by players who get more circulation than I do that I am widely perceived as a kind of mythic figure, a mysterious wizard in his magical tower. Rumor and hearsay have spread word of my supposed opinions on matters of MUD policy. The effect is that players are often afraid to contact me for fear of capricious retaliation at their presumption.

While I find this situation disturbing and wish that I had more time to spend out walking among the 'mortal' members of the LambdaMOO community, I am told that player fears of wizardly caprice are jusified on certain other MUDs. It is certainly easy to believe the stories I hear of MUD wizards who demand deference and severely punish those who transgress; there is a certain ego boost to those who wield even simple administrative power in virtual worlds, and it would be remarkable indeed if no one had ever started a MUD for that reason alone.

2.2 Observations about small groups

MUD conversation. The majority of players spend most of their active time on MUDs in conversation with other players. The mechanisms by which those conversations get started generally mirror those that operate in real life, though sometimes in interesting ways.

Chance encounters between players exploring the same parts of the database are common and almost always cause for conversation. As mentioned above, the anonymity of MUDs tends to lower social barriers and to encourage players to be more outgoing than in real life. Strangers on MUDs greet each other with the same kinds of questions as in real life: "Are you new here? I don't think we've met." The very first greetings, however, are usually gestural rather than verbal: "Munchkin waves. Lorelei waves back."

The @who (or WHO) command on MUDs allows players to see who else is currently connected and, on some MUDs, where those people are. An example of the output of this command appears in Figure 5. This is, in a sense, the MUD analog for scanning the room in a real-life gathering to see who's present.

Players consult the @who list to see if their friends are connected and to see which areas, if any, seem to have a concentration of players in them. If more than a couple of players are in the same room, the presumption is that an interesting conversation may be in progress there; players are thus more attracted to more populated areas. I call this phenomenon 'social gravity;' it has a real-world

analog in the tendency of people to be attracted to conspicuous crowds, such as two or more people at the door of a colleague's office.

It is sometimes the case on a MUD, as in real life, that one wishes to avoid getting into a conversation, either because of the particular other player involved or because of some other activity one does not wish to interrupt. In the real world, one can refrain from answering the phone, screen calls using an answering machine, or even, in copresent situations, pretend not to have heard the other party. In the latter case, with luck, the person will give up rather than repeat himself more loudly.

Player name	Connected	Idle time	Location
Haakon (#2)	3 days	a second	Lambda's Den
Lynx (#8910)	a minute	2 seconds	Lynx' Abode
Garin (#23393)	an hour	2 seconds	Carnival Grounds
Gilmore (#19194)	an hour	10 seconds	Heart of Darkness
TamLin (#21864)	an hour	21 seconds	Heart of Darkness
Quimby (#23279)	3 minutes	2 minutes	Quimby's room
koosh (#24639)	50 minutes	5 minutes	Corridor
Nosredna (#2487)	7 hours	36 minutes	Nosredna's Hideaway
yduJ (#68)	7 hours	47 minutes	Hackers' Heaven
Zachary (#4670)	an hour	an hour	Zachary's Workshop
Woodlock (#2520)	2 hours	2 hours	Woodlock's Room

Total: 11 players, 6 of whom have been active recently.

Sample output from the @who command Figure 5

The mechanisms are both similar and interestingly different on MUDs. It is often the case that MUD players are connected but idle, perhaps because they have stepped away from their terminal for a while. Thus, it often happens that one receives no response to an utterance in a MUD simply because the other party wasn't really present to see it. This commonly understood fact of MUD life provides for the MUD equivalent of pretending not to hear. I know of players who take care after such a pretense not to type anything more to the MUD until the would-be conversant has left, thus preserving the apparent validity of their excuse.

Another mechanism for avoiding conversation is available to MUD players but not to people in real-life situations. Most MUDs provide a mechanism by which each player can designate a set of other players as 'gagged'; the effect is that the gagging player will not hear anything said by someone they've gagged. There is generally no mechanism by which the gagged player can tell a priori that someone is gagging them; indeed, unless the gagged player attempts to address the gagging player directly, the responses from the other players in the room (who may not be gagging the speaker) may cause the speaker never even to suspect that some are not hearing them.

We provide a gagging facility on LambdaMOO, but it is fairly rarely used; a recent check revealed only 16 players out of almost 1500 who have non-empty gagging sets. The general feeling appears to be that gagging is quite rude and is only appropriate (if ever) when someone persists in annoying you in spite of polite requests to the contrary. It is not clear, though, quite how universal this feeling is. I am given to understand that gagging is much more commonly employed on certain other MUDs.

The course of a MUD conversation is remarkably like and unlike one in the real world. Participants in MUD conversations commonly use the emote command to make gestures, such as nodding to urge someone to continue, waving at player arrivals and departures, raising eyebrows, hugging to apologize or soothe, etc. As in electronic mail (though much more frequently), players employ standard 'smiley-face' glyphs (e.g., ':-)', ':-(', and ':-|') to clarify the 'tone' with which they say things. Utterances are also frequently addressed to specific participants as opposed to the room as a whole (e.g., "Munchkin nods to Frebble. 'You tell 'em!'").

The most obvious difference between MUD conversations and those in real life is that the utterances must be typed rather than simply spoken. This introduces significant delays into the interaction and, like nature, MUD society abhors a vacuum.

Even when there are only two participants in a MUD conversation, it is very rare for only one thread of discussion to exist; during the pause while one player is typing a response, the other player commonly thinks of something else to say and does so, introducing at least another level to the conversation, if not a completely new topic. These multi-topic conversations are a bit disorienting and bewildering to the uninitiated, but it appears that most players quickly become accustomed to them and handle the multiple levels smoothly. Of course, when more than two players are involved, the opportunities for multiple levels are only increased. It has been pointed out that a suitable punishment for truly heinous social offenders might be to strand them in a room with more than a dozen players actively conversing.

This kind of cognitive time-sharing also arises due to the existence of the page command. Recall from the introduction that this command allows a player to send a message to another who is not in the same room. It is not uncommon, especially for wizards, whose advice is frequently sought by 'distant' players, to be involved in one conversation 'face to face' and one or two more being conducted via page. Again, while this can be overwhelming at first, one can actually come to appreciate the fact that it relieves one of the tedious long pauses waiting for a fellow conversant to type.

The somewhat disjointed nature of MUD conversations, brought on by the typing pauses, tends to rob them of much of the coherence that makes real-life conversants resent interruptions. The addition of a new conversant to a MUD conversation is much less disruptive; the 'flow' being disrupted was never very strong to begin with. Some players go so far as to say the interruptions are simply impossible on MUDs; I think that this is a minority impression, however. Interruptions do exist in MUDs;

they are simply less significant than in real life.

Other small-group interactions. I would not like to give the impression that conversation is the only social activity on MUDs. Indeed, MUD society appears to have most of the same social activities as real life, albeit often in a modified form.

As mentioned before, PernMUSH holds large-scale, organized social gatherings such as 'hatchings,' and they are not alone. Most MUDs have at one time or another organized more or less elaborate parties, often to celebrate notable events in the MUD itself, such as an anniversary of its founding. To the best of my knowledge, we have had only one or two large-scale parties so far on LambdaMOO; if there were any more, I was not invited!

One of the more impressive examples of MUD social activity is the virtual wedding. There have been many of these on many different MUDs, but none yet announced on LambdaMOO [5]. I have never been present at such a ceremony, but I have read logs of the conversations at them. As I do not know any of the participants in the ceremonies I've read about, I cannot say much for certain about their emotional content. As in real life, they are usually very happy and celebratory occasions with an intriguing undercurrent of serious feelings. I do not know and cannot even speculate about whether or not the main participants in such ceremonies are usually serious or not, whether or not the MUD ceremony usually (or even ever) mirrors another ceremony in the real world, or even whether or not the bride and groom have ever met outside of virtual reality.

The very idea, however, brings up interesting and potentially important questions about the legal standing of commitments made only in virtual reality. I suspect that our real-world society will have to face and resolve these issues in the not-too-distant future.

MUD players also tend to be interested in games and puzzles, so it is no surprise that many real-world examples have been implemented inside MUDs. What may be surprising, however, is the extent to which this is so.

On LambdaMOO alone, we have machine-mediated Scrabble, Monopoly, Mastermind, backgammon, Ghost, chess, go, and reversi boards. These attract small groups of players on occasion but generally have little to offer, if anything, over their real-world counterparts except perhaps a better chance of finding an opponent.

More interesting are the other kinds of games imported into MUDs from real life, the ones that might be far less feasible in a non-virtual reality. A player on LambdaMOO, for example, implemented a facility for holding food fights. Players throw food items at each other, attempt to duck oncoming items, and, if unsuccessful, are 'splattered' with messes that cannot easily be removed. After a short interval, a semi-animate 'Mr. Clean' arrives and one by one removes the messes from the participants, turning them back into the food items from which they came, ready for the next fight.

Another player on LambdaMOO created a trainable Frisbee, which any player could teach to do tricks when they threw or caught it. Players who used the Frisbee seemed to take great pleasure in trying to outdo each other's trick descriptions. I have also heard of MUD versions of paint-ball combat and fantastical games of Capture the Flag.

2.3 Observations about the MUD community as a whole

MUD communities tend to be very large in comparison to the number of players actually active at any given time. On LambdaMOO, for example, we have between 350 and 450 players connecting in any week but rarely more than about 35 simultaneously. A good real-world analog might be a bar with a large number of 'regulars,' all of whom are transients without fixed schedules.

The continuity of MUD society is thus somewhat tenuous; many pairs of active players exist who have never met each other. In spite of this, MUDs do become true communities after a time. The participants slowly come to consensus about a common (private) language, about appropriate standards of behavior, and about the social roles of various public areas (e.g., where big discussions usually happen, where certain 'crowds' can be found, etc.).

It is at this more macroscopic scale that I feel least qualified to make reliable observations, but I do have one striking example of societal consensus having concrete results on LambdaMOO.

From time to time, we wizards are asked to arbitrate disputes among players concerning what is or is not appropriate behavior. My approach has usually been to ask a number of other players for their opinions and to present the defendant in the complaint with a précis of the plaintiff's grievance, always looking for the common threads in their responses. After many such episodes, I was approached by a number of players asking that a written statement on LambdaMOO 'manners' be prepared and made available to the community. I wrote up a list of those rules that seemed implied by the set of arbitrations we had performed and published them for public comment. To date, very little comment has been received; the groups of players I've asked generally agree that the rules reflect their own understandings of the common will. For the curious, I have included our list of

```
o Be polite.  Avoid being rude.
o 'Revenge is ours', sayeth the wizards.
o Respect other players' sensibilities.
o Don't spoof.
o Don't shout.
o Only teleport your own things.
o Don't teleport silently.
o Don't hog the server.
o Don't waste object numbers.
```

The main points of LambdaMOO manners Figure 6

rules in Figure 6; the actual 'help manners' document goes into some detail about each of these points [6].

It should be noted that different MUDs are truly different communities and have different societal agreements concerning appropriate behavior. There even exist a few MUDs where the only rule in the social contract is that there is no social contract. Such 'anarchy' MUDs have appeared a few times in my experience and seem to be quite popular for a time before eventually fading away.

3 The Prospects for Mudding in the Future

> The clumsy system of public gatherings had been long since abandoned; neither Vashti nor her audience stirred from their rooms. Seated in her arm-chair, she spoke, while they in their arm-chairs heard her, fairly well, and saw her, fairly well.
> *E.M. Forster*

A recent listing of Internet-accessible MUDs showed approximately 150 active around the world, mostly in the United States and Scandinavia. A conservative guess that these MUDs average 100 active players each gives a total of 15,000 active mudders in the world today. This is almost certainly a significant undercount already, and the numbers appear to be growing as more and more people gain Internet access.

In addition, at least one MUD-like area exists on the commercial CompuServe network, and I have seen a demonstration of a half-graphical, half text-based virtual reality with 10,000 users in Japan.

I believe that text-based virtual realities and wide-area interactive 'chat' facilities are becoming more and more common and will continue to do so for the foreseeable future. Like CB radios and telephone party lines before them, MUDs seem to provide a necessary social outlet.

The MUD model is also being extended in new ways for new audiences. For example, I am currently involved in adapting the LambdaMOO server for use as an international teleconferencing and image database system for astronomers. Our plans include allowing scientists to give online presentations to their colleagues around the world, complete with 'slides' and illustrations automatically displayed on the participants' workstations. The same approach could be used to create online meeting places for workers in other disciplines as well as for other non-scientific communities. I do not believe that we are the only researchers planning such facilities. In the near future (a few years at most), I expect such specialized virtual realities to be commonplace, an accepted part of at least the academic community.

Some of my colleagues have suggested that the term 'text-based virtual reality' is an oxymoron, that 'virtual reality' refers only to the fancy graphical and motion-sensing environments being worked on in many places. They go on to predict that these more physically involving systems will supplant the text-based variety as soon as the special equipment becomes a bit more widely and cheaply available. I do not believe that this is the case.

While I agree that the fancier systems are likely to become very popular among those who can afford them, I believe that MUDs have (at least) two enduring advantages that will save them from obsolescence:

- The equipment necessary to participate fully in a MUD is significantly cheaper, more widely available, and more generally useful than that for the fancy systems; this is likely to remain the case for a long time to come.
- It is substantially easier for players to give themselves vivid, detailed, and interesting descriptions (and to do the same for the descriptions and behavior of the new objects they create) in a text-based system than in a graphics-based one. I find it difficult to believe that a graphics-based system will be able to compete with text on the metric of believable detail per unit of effort expended; this is certainly the case now, and I see little reason to believe it will change in the near future.

4 Conclusions

> Vashti was seized with the terrors of direct experience. She shrank back into her room, and the wall closed up again.
> *E.M. Forster*

The emergence of MUDs has created a new kind of social sphere, both like and radically unlike the environments that have existed before. As they become more popular and more widely accessible, it appears likely that an increasingly significant proportion of the population will become familiar with mudding and perhaps become frequent participants in text-based virtual realities.

It therefore behooves us to begin to try to understand these new societies, to make sense of these electronic places where we'll be spending time, doing business, and seeking pleasure.

■

Acknowledgements

I was originally prodded into writing down my mudding experiences by Eric Roberts. In trying to get a better handle on an organization for the material, I was aided immeasurably by my conversations with Francoise Brun-Cottan; she consistently brought to my attention phenomena that I had become too familiar with to notice. I must also give credit to the LambdaMOO players who participated in my online brainstorming session; their ideas, experiences, and perceptions provided a necessary perspective to my own understanding.

Notes

[1] Forster, E.M., "The Machine Stops". In Ben Bova, editor, *The Science Fiction Hall of Fame*, Vol. IIB, Avon, 1973. Originally in E.M. Forster, The Eternal Moment and Other Stories, Harcourt Brace Jovanovich, 1928.

[2] Raymond, Eric S., editor, *The New Hacker's Dictionary*. MIT Press, 1991.

[3] In fact, these two commands are so frequently used that single-character abbreviations are provided for them. The two example commands would usually be typed as follows:

```
"Can anyone hear me?
:smiles.
```

[4] The 'MOO' in 'LambdaMOO' stands for 'MUD, Object Oriented.' The origin of the 'Lambda' part is more obscure.

[5] This may change very soon; two players who first met on LambdaMOO and recently did so again in real life have asked me (in my wizardly persona) to officiate at their MUD wedding.

[6] The rule concerning 'spoofing' may mystify some readers. On a MUD, spoofing is the practice of arranging (via programming or trickery) for messages to appear either without attribution or with a misleading one. For example, a player Munchkin might arrange for everyone in a room to see the message

```
Frebble thumbs his nose at Lorelei.
```

without any corresponding intent on Frebble's part. Munchkin would be guilty of spoofing.

Pavel Curtis has been a member of the research community at Xerox PARC since 1983, during which time he has worked on a variety of projects mostly related to the design and implementation of programming languages.

ACCESS TO MUDs:

LambdaMOO can be reached at the Internet host lambda.parc.xerox.com (the numeric address is 13.2.116.36), port 8888. On a UNIX machine, the command

```
telnet lambda.parc.xerox.com 8888
```

or `telnet 13.2.116.36 8888`

will suffice to make a connection. Once connected, feel free to page me; I connect under the names 'Haakon' and 'Lambda'.

The USENET news group rec.games.mud periodically carries comprehensive lists of publicly available, Internet-accessible MUDs, including their detailed network addresses. Some of which are:

Name	Numeric Address	Port
CyberWorld	192.43.199.33	3000
Frontier	130.179.168.77	9165
Middle-Earth	130.209.240.66	3000
PernMUSH	18.70.0.216	4201

To connect to these MUDs use the 'telnet' command as shown above.

There are also a number of clients available. A client is a program that a user can run and use to connect to a MUD in order to improve the MUD interface. Most clients include features such as word wrapping, separating your input text from the MUD's output, and macros. A number of clients are availble by anonymous ftp from the following sites:

piggy.ucsb.edu (128.111.72.50) : /pub/mud/clients
moebius.math.okstate.edu (139.78.10.3) : /pub/muds/clients

```
**************************
*  Welcome to LambdaMOO!  *
**************************

Type `create  <character-name> <password>' to create a new character,
     `connect <character-name> <password>' to connect to an existing one,

connect Guest

*** Connected ***
The Coat Closet
The closet is a dark, cramped space. It appears to be very crowded in here; you keep bumping into what feels like
coats, boots, and other people (apparently sleeping). One useful thing that you've discovered in your bumbling
about is a metal doorknob set at waist level into what might be a door.

open door
You open the closet door and leave the darkness for the living room, closing the door behind you so as not to wake
the sleeping people inside.
The Living Room
It is very bright, open, and airy here, with large plate-glass windows looking southward over the pool to the
gardens beyond. On the north wall, there is a rough stonework fireplace, complete with roaring fire. The east and
west walls are almost completely covered with large, well-stocked bookcases. An exit in the northwest corner leads
to the kitchen and, in a more northerly direction, to the entrance hall. The door into the coat closet is at the
north end of the east wall, and at the south end is a sliding glass door leading out onto a wooden deck. There are
two sets of couches, one clustered around the fireplace and one with a view out the windows.You see a newspaper,
Welcome Poster, README for New MOOers, The Daily Whale, A Tourist's Guide to LambdaMOO, a cuckoo clock on the
mantle, Cockatoo, zoologist, Mystic Bauble, A Vat of Chocolate Syrup, Silver handcuffs, A pair of rubber ears,
FLOWER, Thrust-o-matic, and Lucky fuck tab here.
Frand, Yoyoma, Alice, Guest, and E.J. are here.

Yoyoma says, "Hello, Guest."
```

• • •

NEWSFLASH

TELECOM:

INMARSAT, an organization founded by 64 countries to provide satellite communications for ocean-going vessels, has announced plans to launch a global mobile satellite communications system. This system, called **Project 21**, would allow go-anywhere phone service by the end of the decade at a reasonable cost. Inmarsat estimates that a handheld voice phone would cost around $1,000 and that service would cost less than $1 a minute. Project 21 will directly compete with Motorola's project Iridium...

Researchers have reported that exposing fiber optic cables to high temperature increases can result in a **fuse effect**, "which effectively ruins the fiber as a medium for transmitting light." Although this finding will have little impact on conventional fiber optic installations, it is an important warning for sites where fiber is used in critical applications...

AT&T said that its worldwide **network set a new record** by handling 157.8 million calls on December 6th with all but 211 calls getting through on the first try. The calling volume on an average business day is 127 million calls... AT&T officially exited the telegraph business, making the last letter of their name a historical curiosity...

According to most of the regulators and legislators in attendance at the U.S. Telephone Association's annual conference, regional Bell Company **monopolies will be dissolved** in favor of competition within the local loop by 1999... At a recent symposium, telecommunications experts argued that fiber should not be run to the home due to high costs and low benefits. Although some did argue that fiber is necessary in order to provide the bandwidth needed for future multimedia computer applications, the cost for **ubiquitous fiber** installation, estimated at $200 billion, may be prohibitive...

As Advanced Network & Services, Inc. (ANS) begins to upgrade **NSFNET** to T-3 in order to allow gigabit speeds, users have begun to complain about several recent outages. Critics accuse ANS of using unproven technology by agreeing to use prototype T-3 routers by IBM.. However, with the traffic volume on the Internet growing at a rate of 250% per year (currently 11 billion packets are sent per month), there is little disagreement that the migration to T-3 must be accomplished as soon as possible...

AT&T's network set a new record by handling 157.8 million calls with all but 211 getting through.

It was originally feared that the telecommunications bottleneck between East and West would be difficult to solve due to **East Germany's** outdated equipment. However, by November of this year 55% of calls from West to East Germany were going through, compared to 5% last year... Nonetheless, due to the strain that the telephone system is under, Germany is refusing to break up the Bundespost monopoly as was requested by the EEC...

A number of companies have said that they are unwilling to make their internal e-mail directories be public for fear of "junk e-mail" and loss of privacy. This is a major blow to the **Directory Forum**, a group of information service providers founded in 1990 with the goal of establishing a global public directory service based on X.500, the CCITT standard for directory services. In response, the Directory Forum has announced plans to create a "Bill of Rights" for users of their service which would protect individuals' and companys' privacy...

Nahshon Even-Chaim, a 20-year old computer science student, is on trial in Melbourne's Magistrates' Court on charges of gaining unauthorized access to one of CSIRO's (Australia's government research institute) computers and 47 counts of misusing Australia's Telecom phone system for unauthorized access to computers at various US institutions. The sites include universities, NASA, Lawrence Livermore Labs, and Execucom Systems Corp. of Austin, Texas, where it is alleged he destroyed important files, including the only inventory of the company's assets....

The General Accounting Office (GAO) found a total of 68 computer and network security and control problems at five of the nation's six major exchanges during reviews it conducted this past year for the **Securities and Exchange Commissions.** The report claimed that the lack of adequate controls at the five stock markets could impair their ability to maintain continuous service, protect critical computer equipment and operations, and process correct information. The exchanges with the greatest number of problems were the Midwest (24), Pacific (18), and Philadelphia (18) exchanges, all of which were faulted for their inadequate risk analysis...

COMPUTERS:

DIMENSION Technologies Inc. announced the first commercial display able to deliver true stereoscopic **3-D images** without the need for special glasses. The screen consists of two active-matrix LCD displays side by side. The columns alternate in displaying the image so that for 1/30th of a second the left eye sees one column. The column then darkens and the opposite column lights up for the right eye. Because the after-image remains, the brain combines the two sets of images to form one image that appears to have depth. More than one person can view the 3-D image at the same time. The screen currently provides 4,096 colors and lists for $10,000...

Scientists at Iterated Systems Inc. have achieved a record-setting **compression** ratio of 2,456:1 in reducing a color image. The compression was done by using fractal mathematics to describe patterns in the picture. In this way, only an equation a few bytes long needs to be stored in order to represent an area of the picture. This method appears to be far more efficient than the current Joint Photographic Experts Group (JPEG) standard. A further advantage of using fractal equations is that the compression method is resolution independent, allowing a compressed picture to be decompressed to any resolution...

A new model of **neuron behavior,** developed at Los Alamos, confirms that noise plays a crucial role in natural information processing systems. Researchers found that a model of a neuron would only reproduce experimental data from live neuron studies when a noise factor was added. Scientists had previously believed that noise was simply tolerated by neurons and not actually necessary. Scientists now hypothesize that noise is necessary because it provides a stabilizing factor to the dynamic system of a neuron...

While most flat panel researchers have turned away from **CRT technology** in favor of LCDs and other display technologies, French researchers have succeeded in sharply shrinking the size of CRTs. By using vacuum microelectronics, the French team has developed a 6-inch CRT that is only 2 mm thick. The researchers also believe that the technology can be scaled up to provide displays as large as one meter...

Japanese scientists demonstrated a new computer which represents the current state of the **fifth-generation project**. The fifth-generation project was launched in 1982 by MITI with the goals of creating a computer that could understand natural speech and respond to imprecise information, using its own knowledge database. In order to build such a computer the Japanese rejected the classical Von Neumann model in favor of a parallel computer which could effectively execute programs written in logic-based languages such as PROLOG. Their new computer, the PIM, has 1000 processors which together can perform a record 200 million logical inferences per second. Researchers in Australia and Japan are now working together to develop software for the machine...

A new model of neuron behavior confirms that noise plays a crucial role in natural information processing.

Sony Corp. demonstrated a **holographic storage** system at the Japan Electronics Show. The apparatus stores holographic images directly on a CD platter rather than storing digitized information that can be reconstructed later as a holographic image. The system works by beaming a laser onto the CD. As the platter rotates about its central axis, stored images come into range of the illuminating laser beam, producing a series of still 3-D images...

SGS-Thomson announced plans to make ICs which incorporate **fuzzy logic**. This will allow system developers, who previously had to implement fuzzy logic in software, to use fuzzy logic in time-critical applications. For example, a number of European car manufacturers are working on fuzzy control for automotive engines. Analysts believe that the worldwide market for fuzzy logic semiconductors may total $10 billion by year 2000...

A study by Dataquest, Inc. found that the rate of **virus infections** is growing exponentially. 40% of the users surveyed said that they had encountered a virus during the 3rd quarter this year, up from 25% during the 2nd quarter, and 19% in the first quarter. The study also found that the most common viruses were Stoned and Jerusalem and that the likelihood of having a virus disaster increases with the level of networking...

BIOTECH:

JOHN E. Botzolakis, a former **Parke-Davis** senior scientist, pleaded guilty to charges that he sold the classified formulas of two drugs to the former vice president of American Therapeutics for $14,000 ...

Researchers at City College of New York and at UC Berkeley have shown that the initial chemical change in the **human eye** in response to light occurs in 200 femtoseconds. By beaming extremely short pulses of laser light, the scientists were able to watch as a chemical bond in the protein rhodopsin twisted in response to the absorption of a photon. However, researchers disagree about what happens after this initial reaction. Scientists at City College contend that there is a second stage which lasts 3 picoseconds while the UC Berkeley team argues that this is merely the time when the compound rids itself of excess energy...

Scientists at the University of Arizona were able to trigger the **tanning** of skin by daily subcutaneous injections of a synthetic hormone. In a study on 16 volunteers the skin of the men began to darken within 12 days of the injections. Further tests will be needed to determine if the process has any ill effects...

States across the US are creating **genetic data banks** where DNA samples from convicted criminals are stored. Thirteen states now have laws which allow police to collect DNA samples from convicts. Originally this information was collected specifically to solve rape cases, but this has broadened considerably. In Iowa, DNA samples can be taken even from those convicted of minor offenses. Because it is difficult to match DNA and because it is not unique to each individual (identical twins have identical DNA material), a number of scientists at the National Institute of Health (NIH) have questioned the ethics of taking DNA samples... Relatedly, the Army has announced plans to establish a database that would store "DNA dog tags" for every member of the armed services. Because the devastating force of even conventional warfare often leaves few remains, identification can be problematic. But matching DNA extracted from a single hair follicle, blood sample, or almost any body fluid against the DNA database would allow for accurate identification...

Two new **theories of aging** based on specific gene activity have been proposed. Researchers at The University of Texas presented data showing that aging is partially due to a loss of acute-phase response in the liver. Meanwhile, scientists at the University of Arkansas found that

over-expression of genes related to inhibition of cell growth, blood vessel formation, and blood clotting occurred in a patient with Werner Syndrome. Werner Syndrome is an extremely rare disease which is characterized by premature aging...

At the recent April conference of Federation of American Societies for Experimental Biology, scientists with **Trans Time Inc.** reported a reproducible method for restoring strong rhythmic EKG signals along with heart beats from cryoprotected/frozen/thawed/reperfused hamsters. These hamsters were frozen overnight to between -1.6 to -2.2 deg. C. Since then, the scientists have restored heart beats and EKG signals from hamsters frozen to as low as -3.5 deg. C overnight. The restoration of this physiological function, which involves the coordinated participation of millions of cardiac cells (myocytes, nodal cells and Purkinje cells) indicates we are learning how to reduce freezing damage, a major obstacle of reversible cryonic suspension...

Regeneron was granted exclusive rights for the newly-discovered nerve growth factor NT-4.

The U.S. Supreme Court refused to hear Genetics Institute's appeal to overturn a lower-court decision which invalidated the GI patent for erythropoietin, handing all patent rights to **Amgen.** Professor Laurence Tribe of Harvard Law School protested that the lower-court ruling threatens a fundamental premise of American patent law. Tribe contended that concealing the best mode of implementing one's invention at the time of patent breaks the "social bargain" in allowing a 17-year monopoly...

RECENT BIOTECH PATENTS

Regeneron was granted exclusive worldwide rights for a newly discovered nerve growth factor, neurotrophin-4 (NT-4)... **Oncor** received a patent for a new DNA-amplification chemistry known as RAMP. The technology makes multiple DNA copies of a single gene, allowing detection and analysis of small amounts of DNA... **Lidak Pharmaceuticals** received a patent for "large multivatlent immunogen", a tumor immunotherapy which activates special cells which can destroy cancerous or virally infected cells... **Inteneuron Pharmaceuticals** was assigned a patent for a new compound for appetite suppression, Phenylpropanolamine modified with tyrosine... **DNA Plant Technology** received a patent for its new "transwitch" technology which gives the ability to switch off expression of a specific gene... **Enzytech** received a patent for its ProLease bio-erodible microspheres which can deliver therapeutic proteins and peptides...

(Information from Bio/Technology.*)*

SPACE PROBES:

As of December 20th 1991, the **Magellan** spacecraft performance is excellent. All systems are nominal, and attitude pointing remains precise. The spacecraft is on orbit #3771 and has completed 3282 radar mapping orbits. It has finished 88% of its second cycle of Venus. A new Radar Control Parameter File will be uplinked to the spacecraft on Monday, 12/23...

PROBE: GALILEO	12/19
DISTANCE: 294 million miles	
SPEED: 33,540 mph	

On October 29, **Galileo's** camera snapped 150 picture of a tiny asteroid called Gaspra as it passed within 1,600 kilometers of the space probe. The pictures sent back have already dramatically increased our state of knowledge about asteroids. Because of problems with the craft's main antenna, scientists originally didn't think that any pictures of the asteroid would be available until December 1992, when the craft swings around Earth again to gain speed on its way to Jupiter. However, due to a stroke of luck, two of the pictures sent back by the small antenna (which takes 80 hours to transmit one picture) contained clear pictures of Gaspra. These images show an irregularly shaped asteroid, measuring about 12 by 20 by 11 kilometers. Gaspra is covered with craters and grooves, leading researchers to believe that Gaspra is the result of a series of catastrophic collisions between larger parent bodies...

Scientists at NASA tried again to unstick the large antenna. The precool portion of the cooling turn was completed on December 13. The spacecraft bus cooled down from 25 degrees C to 18.7 deg. C which is approximately one degree higher than the predicted value. The turn to 165 degrees off-sun was initiated on December 13 at 1426 PST. The spacecraft remained at cooling attitude for approximately 50 hours, at which time the spacecraft was commanded back to five degrees off-sun. After the turn was completed at 2140 PST, sun gate data was collected to determine if an antenna rib was still obscuring the sun gate signal. Data analysis subsequently indicated that the sun gate was still obscured... Another problem occurred on December 17 when Telemetry Channel E-1635 went into alarm, indicating that the magnetometer boom was not deployed. Prior to this time, telemetry from the microswitch indicated that the mag boom was completely deployed. All other spacecraft telemetry indicators suggest the magnetometer boom is still fully deployed. Possible failure modes include the switch, gate and mechanical devices areas; these are being investigated.

PROBE: ULYSSES	12/16
DISTANCE: 441 million miles	
SPEED: 33,000 mph	

Ulysses is currently configured with receiver 2 as the prime unit feed via the high gain antenna and with receiver 1 as backup feed through the low gain antenna. The downlink is provided through EPC2/TWTA2. The 34 meter ground stations are in use to support TTC operations. The spacecraft currently has a spin rate of 4.984 rpm. Tape recorder operations based on recovering data acquired during the out-of-view periods are continuing on a routine, scheduled basis. Experiment reconfigurations have been carried out as required. An average of 97.57% data recovery was achieved during this reporting period. The next Earth pointing manoeuvre will be carried out on January 4th.

(Probe information from NASA bulletins.)

■

SUBSCRIPTION INFORMATION

VOLUME 3.1: The Hacker Issue

- Interviews with John Barlow and Erik Bloodaxe
- Katie Hafner on hackers
- Monique on monitoring phone lines with LMOS
- Conference report on CRYPTO '90
- Notes from the front lines of the drug war

$5

VOLUME 3.2: The Ethics Issue

- Interviews with Brenda Laurel and Bruce Sterling
- John Gilmore on privacy in America
- Debate on scientific ethics
- Mike Perry on 3D graphics
- Kevin Brown on uploading

$5

The current issue is available for $4.

A subscription is $14 for two years (total of 4 issues).

Add 30% for overseas.

325 Ellwood Beach, #3
Goleta, CA 93117
steve@cs.ucsb.edu
805.685.6557

"I think that the human race actually is about some great work that no one really knows the nature of. But we all want to participate in it. My sense of it is that it involves hard-wiring consciousness, creating the collective organism of human consciousness. I don't know why we'd want to do such a thing, but I feel a strange mystical motivation to be part of it. There are plenty of people out there making it happen on a technical level, who are far more adept at that than I am, but who are not giving a lot of thought to the cultural elements. I want to do what I can to make it happen on a human level."

John Barlow,
in *Intertek 3.1*